Vysoká škola báňská – Technická univerzita Ostrava

Fakulta bezpečnostního inženýrství

Katedra bezpečnostních služeb

Bezpečnostní scénáře pro zajištění bezpečného chodu nemocnic

Safety scenarios to ensure the safe running of hospitals

Student: Bc. Vojtěch Mentuz

Vedoucí diplomové práce: Ing. Petr Bitala, Ph.D.

Studijní program: Požární ochrana a průmyslová bezpečnost

Studijní obor: Technická bezpečnost osob a majetku

Termín odevzdání diplomové práce: 16. 4. 2021

Poděkování:

Tímto bych chtěl poděkovat svému vedoucímu práce panu Ing. Petru Bitalovi, Ph.D., za odborné vedení, cenné rady a připomínky při zpracování mé diplomové práce.

Anotace

Bc. MENTUZ, Vojtěch. *Bezpečnostní scénáře pro zajištění bezpečného chodu nemocnic*. Diplomová práce. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství, 2021. 96 stran včetně příloh. Vedoucí práce Ing. Petr Bitala, Ph.D.

Diplomová práce se zabývá návrhem bezpečnostních scénářů popisující logickou součinnost systémů technické ochrany a jejich provázanost s režimovou ochranou pro zajištění bezpečnějšího chodu nemocničních zařízení. Úvodní část práce stručně představuje kategorizaci jednotlivých zdravotnických zařízení na území ČR. Další části práce jsou následně zaměřeny pouze na nemocniční zařízení, ve kterých se na základě jejich charakteristických vlastností předpokládá kritický dopad na funkčnost v rámci vzniku mimořádné události. Na konci teoretické části je popsána celková bezpečnost nemocničních zařízení s hlavním zaměřením na systémy technické a požární ochrany, které se v těchto zařízeních obvykle využívají. Praktická část se na úvod zabývá průzkumem vzniklých bezpečnostních incidentů v nemocnicích a dále se zaměřuje na vytvoření posouzení rizik. Následně definuje základní parametry související s návrhem systémů technické ochrany. Tyto návrhy jsou následně aplikovány u vytváření bezpečnostních scénářů na zvolené mimořádné události. S ohledem na hodnocení rizik jsou scénáře vytvořeny na verbální a fyzické napadení beze zbraně, ozbrojený útok a požár.

Klíčová slova: Zdravotnická zařízení, nemocnice, systémy technické ochrany, bezpečnostní scénáře, ozbrojený útok, požár, fyzické napadení, poplachové zabezpečovací a tísňové systémy, dohledové videosystémy, elektronické systémy kontroly vstupu, elektrická požární signalizace, evakuační rozhlas

Summary

Bc. MENTUZ, Vojtěch. *Safety scenarios to ensure the safe running of hospitals*. Thesis. Ostrava: VŠB – Technical University of Ostrava, Faculty of Safety Engineering, 2021. 96 pages including attachments. Thesis supervisor Ing. Petr Bitala, Ph.D.

The thesis deals with the design of safety scenarios describing the logical dependence of technical protection systems and their interdependence with regime protection to ensure safer operation of medical facilities. The introductory part of the thesis briefly presents the categorization of individual medical facilities in the Czech Republic. Other parts of the thesis are focused only on hospital facilities where a critical impact on functionality in the event of an emergency is assumed, based on their characteristics. The overall safety of hospital facilities with a focus on the technical and fire protection systems normally used in these facilities is described at the end of the theoretical part. The practical part deals with the examination of security incidents in hospitals and focuses on the creation of a risk assessment. It then defines the basic parameters related to the design of technical protection systems. These suggestions are then applied to creating security scenarios for selected emergencies. The scenarios are created with regard to risk assessment for verbal and physical assault without a weapon, armed attack and fire.

Keywords: Medical facilities, hospitals, technical protection systems, security scenarios, armed attack, fire, physical assault, intrusion and hold-up alarm systems, video surveillance systems, electronic access control systems, fire alarm systems, voice alarm

Obsah

Seznam zkratek

ČSN	Česká státní norma
DPPC	Dohledové poplachové a přijímací centrum
EPS	Elektrická požární signalizace
ESKV	Elektronické systémy kontroly vstupu
FO	Fyzická ochrana
FOs	Fyzická ostraha
MK	Magnetický kontakt
MU	Mimořádná událost
MVČR	Ministerstvo vnitra České republiky
MZP	Mechanické zábranné prostředky
NVS	Nástražné výbušné systémy
PBZ	Požárně bezpečnostní zařízení
PZTS	Poplachové zabezpečovací a tísňové systémy
SHZ	Stabilní hasící zařízení
STO	Systémy technické ochrany
TH	Tísňový hlásič
VSS	Dohledové videosystémy
WHO	Světová zdravotnická organizace
ZOTK	Zařízení pro odvod tepla a kouře

Úvod

V oblasti fyzické ochrany objektů jsou zdravotnická zařízení v současné době středem pozornosti, a to z důvodu událostí, které se staly v nedávné minulosti. Jedná se především o kybernetické útoky na informační systémy nebo fyzické útoky na zdravotnický personál, pacienty či návštěvníky. Příkladem událostí tohoto druhu může být případ střelby ve Fakultní nemocnici Ostrava, která se stala v prosinci roku 2019. Ta vyvolala vlnu otázek a pochybností, zda jsou v těchto zařízeních nastavena dostatečná bezpečnostní opatření a jestli jsou tato opatření efektivně implementována.

Zdravotnická zařízení zařazujeme mezi zařízení kritické infrastruktury, které můžeme dle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (neboli krizový zákon), ve znění pozdějších předpisů, definovat jako prvek, nebo systém prvků, kdy při narušení tohoto systému může dojít k ohrožení bezpečnosti státu, ekonomiky nebo k narušení schopnosti zajistit bezpečnost obyvatel a ochranu života a zdraví osob [49]. Vybraná zařízení poskytující zdravotní péči lze také zařadit mezi tzv. měkké cíle. Tento termín je využíván pro označení lokalit se zvýšeným rizikem vzniku bezpečnostních incidentů z důvodu vysoké koncentrace osob a relativně nízkým stupněm zabezpečení. Zmíněné vlastnosti vytvářejí pro pachatele atraktivní cíl pro provedení případného útoku. Útoky mohou být směřovány jak na majetkové hodnoty, tak na přítomné osoby. Tato specifická zařízení by proto měla zajišťovat prostředí s přijatelnou mírou bezpečnosti s ohledem každodenní práci s pacienty rozličného typu nebo z důvodu skladování a manipulace různých medikamentů.

Míra bezpečnosti zdravotnických zařízení může mít nepochybně určitý vliv na proces uzdravování pacientů. Pocit nebezpečí může působit na lidskou psychiku, popř. na fyziologické pochody v organismu, což může výrazným způsobem negativně ovlivňovat úspěšnost léčby. Pokud se pacient ocitne v prostředí, ve kterém se necítí bezpečně a nemůže zde dělat to, co je pro něj přirozené, může to mít za následek zvyšování hladiny nervozity, nejistoty a stresu.

Lze říci, že určitou bezpečnostní politiku má dnes implementovanou každé zdravotnické zařízení. Její rozsah je dán typem zařízení, dispozičním řešením, ale také jeho finančními možnostmi. Proto se ve zmíněných zařízeních setkáváme s rozdílným rozsahem využívaných bezpečnostních opatření, která se obvykle zaměřují na fyzickou ostrahu,

systémy technické či požární ochrany a režimovou ochranu. Neméně důležitým procesem je také implementace vyhovujících bezpečnostních pravidel pro zaměstnance, návštěvy a osoby, které poskytují určité služby danému zdravotnickému zařízení (např. dodavatelé). Nicméně ani využití nejmodernější technologie nemusí umožnit realizaci optimálních bezpečnostních opatření. Dnes existuje mnoho normativních a právních předpisů, které definují, jakým způsobem a v jakém rozsahu mají být zmíněná opatření implementována, ale je zde zjevná absence normovaného postupu a doporučení popisující propojení a správné nastavení těchto opatření umožňující plné využití potenciálu systémů technické a požární ochrany spolu s fyzickou ostrahou.

Teoretická část práce se v úvodu zabývá kategorizací a popisem zdravotnických zařízení na území ČR s následným zaměřením na nemocniční zařízení, které lze z pohledu bezpečnosti považovat za kritické. Následující část práce se věnuje členění a stručnému popisu bezpečnostních opatření z oblasti fyzické ochrany, která jsou nyní v nemocničních zařízeních běžně implementována. Jedná se o stručnou charakteristiku fyzické ostrahy, režimové ochrany a systémů technické a požární ochrany spolu s dalšími interními systémy.

V úvodu praktické části je provedeno posouzení rizik pro nemocniční zařízení, to obsahuje identifikaci, analýzu a hodnocení rizik. Dále jsou zde navrženy základní požadavky na rozsah instalace systémů technické a požární ochrany. Požadavky jsou následně reflektovány v hlavní části práce, která předkládá návrhy bezpečnostních scénářů vedoucí k zajištění bezpečného chodu nemocnic. Scénáře popisují efektivní součinnost a propojení jednotlivých systémů technické a požární ochrany spolu s režimovou ochranou a fyzickou ostrahou jako reakci na vzniklou mimořádnou událost, aby případné důsledky na životech, zdraví přítomných osob a majetku byly minimální.

1 Rešerše literatury

Před započetím procesu zpracování diplomové práce byla provedena rešerše literárních zdrojů, studií, právních a normativních předpisů, které se zabývají problematikou fyzické ochrany zdravotnických zařízení.

1.1 Literatura

W. YORK, Tony a Don MACALISTER. *Hospital and Healthcare Security – sixth edition*. 6. vydání, 2015, ISBN 978-0-12-420048-7

Tato publikace popisuje současný stav zabezpečení zdravotnických zařízení v oblasti bezpečnosti dat, ochrany soukromí pacientů, násilí vyvolaného pacienty a celkovou připraveností na mimořádné události. Dále publikace uvádí odborné poznatky z oblasti designu a nouzového řízení. V první části práce se autor zabývá popisem zdravotnických zařízení, jejich kategorizací, typy nemocnic, zaměstnaností atd. V další části publikace popisuje bezpečnost zdravotnických zařízení, vývoj zabezpečení, základní bezpečnostní programy, plánování bezpečnostního managementu, školení, rozvoj bezpečnostních pracovníků apod.

ŠKRLA, Petr a Magda ŠKRLOVÁ. *Řízení rizik ve zdravotnických zařízení*. Praha: Grada publishing, 2008. ISBN 978-80-247-6377-4

Kniha prezentuje integraci výsledků metaanalýzy přístupných studií v oblasti bezpečnosti ve zdravotnických zařízeních. V publikaci jsou vysvětleny pojmy v oblasti řízení rizik a jaký je cíl řízení rizik. Dále je v publikaci popsáno řízení rizik z perspektivy lékařů, ošetřovatelského personálu, pacientů, stravovacího provozu, HTS a personalisty.

1.2 Studie

Madeleine Estryn-Behar, Beatrice van der Heijden, Donatella Camerino, Clementine Fry, Olivier Le Nezet, Paul Maurice Conway, Hans-Martin Hasselhorn, the NEXT Study group, *Violence risks in nursing—results from the European 'NEXT' Study*. Occupational Medicine, Květen 2008, 107-114.

Studie se zaměřovala na identifikaci násilí v ošetřovatelství a poskytnutí základu pro zajištění vhodné intervence. Dotazník byl zaslán zdravotním sestrám z deseti zemí Evropské unie. Zhodnocené dotazníky byly použity k posouzení souvislosti mezi frekvencí násilí, faktory souvisejícími s týmovou prací a dalšími faktory.

Babiarczyk, B., Turbiarz, A., Tomagová, M., Zeleníková, R., Önler, E., and Sancho Cantus, D. (2020). *Reporting of workplace violence towards nurses in 5 European countries – a cross-sectional study*. International Journal of Occupational Medicine and Environmental Health, 33(3), 325-338.

Tato studie se zaměřovala na posouzení specifických znaků týkajících se fyzického a nefyzického násilí na pracovišti vůči zdravotním sestrám. Dále se studie snažila identifikovat důvody neohlašování násilí vůči respondentům. Retrospektivní průřezová studie byla provedena v celkem pěti zúčastněných zemích (Polsko, Česká republika, Slovenská republika, Turecko a Španělsko).

1.3 Normativní dokumenty

ČSN EN 50 131 - Poplachové systémy

Tato řada norem stanovuje systémové požadavky a specifikuje nároky na provedení, vlastnosti prvků poplachových zabezpečovacích a tísňových systémů. Požadavky na návrh, projekci, instalaci, provoz a údržbu jsou následně uvedeny v normě ČSN CLC/TS 50131-7.

ČSN EN 50134-1 - Poplachové systémy – Systémy přivolání pomoci

Tato norma patří do souboru norem pod názvem *"Poplachové systémy – Systémy přivolání pomoci"* a specifikuje základní požadavky na systém pro identifikaci, aktivování poplachu, přenos signálu, přijetí a potvrzení poplachu, záznam a obousměrnou hlasovou komunikaci včetně tříd prostředí ovlivňujících návrh systému.

ČSN EN 60 839-11-1 Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu

Norma stanovuje minimální funkčnost, nároky na provozní vlastnosti a techniky zkoušení pro elektronické systémy kontroly vstupu a další její další komponenty používané pro zajištění kontroly fyzického přístupu do objektů, jejich okolí a do chráněných prostor.

ČSN EN 62676 - Dohledové videosystémy pro použití v bezpečnostních aplikacích

Tato norma předepisuje minimální požadavky a doporučení pro dohledové videosystémy, které jsou využívané v bezpečnostních aplikacích. Specifikuje minimální výkonnostní a funkční nároky sjednané v rámci provozních požadavků mezi objednatelem a dodavatelem.

ČSN EN 50849 – Nouzové zvukové systémy

Účelem normy je stanovit technické požadavky na nouzové zvukové systémy, které jsou určeny k informování osob o vzniklé situaci. Přenos informací probíhá prostřednictvím rozhlasových jednotek v několika stanovených oblastech. Norma poskytuje techniky zkoušení a jednotlivé vlastnosti, které jsou potřebné pro specifikaci systému.

ČSN EN 1627 - Dveře, okna, lehké obvodové pláště, mříže a okenice – Odolnost proti vloupání – Požadavky a klasifikace

Norma určuje požadavky a systém klasifikace vlastností a odolnosti proti vloupání u mechanických zábranných prostředků, a to pro dveře, okna, lehké obvodové pláště, mříže a okenice. Dále norma určuje nároky na odolnost stavebních výrobků proti vloupání.

ČSN 34 2710 - Elektrická požární signalizace – Projektování, montáž, užívání, provoz, kontrola, servis a údržba

Norma stanovuje požadavky určuje zásady pro projektování, montáž, užívání, provoz, kontrolu, servis a údržbu pro systém EPS.

ČSN 73 0875 - Požární bezpečnost staveb – navrhování elektrické požární signalizace

Účelem této normy je stanovit požadavky pro navrhování systému elektrické požární signalizace pro nové stavby a při projektování změn stávajících objektů.

2 Zdravotnická zařízení

Ve veřejných publikacích existuje několik definic pojmu zdravotnictví nebo obecně systému péče o zdraví. Například Světová zdravotnická organizace (dále také World Health Organization – WHO) definuje zdravotnictví jako veškeré činnosti, jejichž hlavním úkolem je obnovovat, podporovat a udržovat duševní a fyzické zdraví člověka. Celý systém má zcela jednotný cíl, jehož výstupem je udržování zdraví současné a budoucí populace. [6]

Zmíněná zařízení představují skupinu různých a jedinečných objektů, kde je péče o pacienta primárním úkolem. Mezi tradiční objekty patří např. nemocnice, kliniky, zubní ordinace, nezávislá pohotovostní oddělení, střediska urgentní péče, rehabilitační domácí péče, objekty dlouhodobé lůžkové péče a samostatná chirurgická centra. Každé z těchto zařízení vyžaduje unikátní způsob ochrany zdraví pacientů, personálu, návštěvníků, dodavatelů a ochrany hmotného i nehmotného majetku. Nicméně existují také léčebná zařízení, která vykonávají svou činnost bez častého výskytu pacientů. Jedná se např. o klinická výzkumná centra, ambulantní diagnostická centra nebo krevní banky. [47]

Zdravotnická zařízení jako taková můžeme dělit z hlediska vlastnictví (státní, nebo nestátní), zisku (soukromé, či neziskové organizace), nebo podle právní formy daného zařízení. Jednotlivé kategorie se mohou vzájemně prolínat, čímž ve skutečnosti vzniká velké množství forem zdravotnických zařízení. Možným příkladem mohou být nemocnice, jež můžou být řízené jak státem, tak krajem. Jako další příklad lze uvést zařízení ambulantní péče, které mohou být poskytovány jak fyzickou, tak právnickou osobou. Zásadním dělením zdravotnických zařízení je dané tím, kdo je jejím zřizovatelem. Velká část státem řízených zdravotnických zařízení spadá pod působnost ministerstva zdravotnictví. Jako názorný příklad můžeme uvést fakultní nemocnice, které nad rámec standardních služeb poskytují velmi specializovanou péči. Fakultní nemocnice jsou příspěvkovými organizacemi, které jsou částečně financovány ze státního rozpočtu, ale většinu jejich příjmů tvoří finance za poskytnutou péči. Dalším typem jsou tzv. nestátní zdravotnická zařízení, která jsou zřizována orgány obcí a krajů v rámci své působnosti. Mohou zřizovat nemocnice, léčebná centra, popřípadě jesle. Kraje mají na základě zákona č. 250/2000 Sb., o zdravotnické záchranné službě, ve znění pozdějších předpisů, povinnost zřídit zdravotnickou záchrannou službu, na jejímž chodu se podílí kromě daného krajského úřadu také ministerstvo zdravotnictví. [35]

Zdravotnická zařízení, která jsou ve vlastnictví fyzických nebo právnických osob, se nazývají soukromá zdravotnická zařízení. Jedná se především o různé druhy ambulancí, léčeben, ozdravných center, stacionářů, nemocnic apod. Provozovatelem zmíněných zařízení je tzv. poskytovatel zdravotních služeb. [35]

2.1 Kategorizace zdravotnických zařízení

Na základě celkového přehledu zdravotnických zařízení, který vydal ÚZIS ČR jakožto Národní registr poskytovatelů zdravotních služeb, bylo v roce 2018 v ČR v provozu celkem 32 080 zdravotnických zařízení. V dostupné statistice bylo celkem 60 kategorií zdravotnických zařízení (seznam těchto zdravotnických zařízení je uveden v Příloze č. 1).

V České republice můžeme dle zákona č. 372/2011 Sb., o zdravotních službách, ve znění pozdějších předpisů, rozdělit zdravotní péči na níže uvedené formy: [50]

- ambulantní péče;
- jednodenní péče;
- lůžková péče;
- péče poskytovaná ve vlastním sociálním prostředí pacienta.

Právě oddělení ambulantní a lůžkové péče jsou v nemocničních zařízeních z hlediska bezpečnosti riziková, a to z důvodu poskytování vysokého počtu lůžek pro možnou hospitalizaci pacientů a vyšší kumulaci přítomných osob v rámci ambulantní péče. S ohledem na zmíněný charakter se tyto objekty mohou stát atraktivním cílem potenciálního útočníka a lze předpokládat kritický dopad na společnost s ohledem na omezenou možnost poskytování nezbytné zdravotnické péče v souvislosti se vznikem mimořádné události. Proto se tato diplomová práce v rámci dalšího zkoumání a návrhu specializuje pouze na nemocniční zařízení.

3 Nemocniční zařízení

Nemocniční zařízení jsou velmi významnou součástí celého zdravotnictví. Jejich hlavním cílem a funkcí je poskytování nepřetržité lékařské zdravotnické péče svým pacientům. Jsou zde poskytovány specializované služby, které výrazně napomáhají ke zlepšování zdravotního stavu populace. Nemocnice lze také definovat jako organizace, které mají licenci k poskytování zdravotnické péče a poskytují svým pacientům lůžkové vybavení, stravu a nepřetržitou ošetřovatelskou péči, která je poskytována kvalifikovaným personálem. ([22], [23])

Nemocnice mimo jiné plní i úkoly z hlediska pregraduální a postgraduální výchovy zdravotnického personálu, kdy hovoříme o tzv. fakultních nemocnicích. Definice pojmu fakultní nemocnice je uvedena v zákoně č. 372/2011 Sb., zákon o zdravotních službách, ve znění pozdějších předpisů, definující tento typ zařízení jako státní příspěvkovou organizaci, jejíž zřizovatelskou funkci vykonává ministerstvo. Fakultní nemocnice zajišťuje zdravotnické služby a související výzkumnou nebo vývojovou činnost. Představuje prostředek, pomocí něhož je stát schopen zajistit veškeré klíčové prvky a služby zdravotnického systému. Nejedná se pouze o poskytování rozsáhlého spektra zdravotnických služeb, ale také o zajišťování zabezpečení infrastruktury pro související úkoly, jako je vzdělávání studentů lékařských fakult, výzkumy a vývoj v oblasti zdravotnických služeb a profesní růst zdravotnických pracovníků. Jedná se o základní pilíř zdravotnictví. ([8], [41])

Hlavním úkolem fakultních nemocnic je především: [8]

- poskytování rozsáhlého spektra zdravotnické péče;
- rozvoj center vysoce specializované zdravotnické péče;
- vytváření podmínek pro výzkum a vývoj v oboru zdravotnictví;
- vytváření podmínek pro zajištění výuky a praxe studentů lékařských fakult;
- vytváření podmínek pro zvyšování kvalifikace zdravotnických pracovníků.

3.1.1 Organizační a právní postavení

S ohledem na platné právní předpisy lze organizačně právní postavení nemocnic zařadit jak do veřejného, tak do soukromého sektoru. Nicméně v dnešní době dochází k různým kombinacím vlastnictví nemocnic. [23]

3.1.2 Členění nemocnic

Nemocnice lze dělit dle následujících kritérií:

- Podle institucionální klasifikace: [23]
  - všeobecné nemocnice;
  - ústavy pro mentálně postižené;
  - specializované nemocnice.
- Podle počtu lůžek: [23]
  - do 700 lůžek;
  - nad 700 lůžek;
- Podle typu vlastnictví: [23]
  - ve vlastnictví a správě státu;
  - ve vlastnictví a správě měst a obcí;
  - soukromé nemocnice;
  - nemocnice provozované na neziskovém principu;
  - nemocnice založené na podnikatelském principu.
- Podle ošetřovací doby: [23]
  - nemocnice pro akutní péči;
  - nemocnice pro dlouhodobou péči.
- Podle převažujícího druhu zdravotnické péče: [23]
  - nemocnice specializované;
  - nemocnice všeobecné.
- Podle hospodaření: [23]
  - nemocnice ziskové;
  - nemocnice neziskové.

Akutní lůžková péče

Tato péče je v nemocničních zařízeních poskytována po dobu nezbytnou k provedení nejdůležitějších vyšetření a ošetření nebo po dobu, kdy je možné důvodně očekávat snížení stability zdravotního stavu pacienta vyžadující intenzivní lékařskou péči. Péče je poskytována při selhávání základních životních funkcí pacientů nebo při náhlém zhoršením chronické nemoci. [23]

Základními obory akutní lůžkové péče: [23]

- vnitřní lékařství;
- chirurgie;
- pediatrie;
- gynekologie a porodnictví.

Následná lůžková péče

Tzv. následná lůžková péče je poskytována pacientům, u kterých byla stanovena diagnóza a došlo k úspěšnému zvládnutí akutního ohrožení zdravotního stavu. U těchto pacientů se neočekává zhoršení stability zdravotního stavu, které by vyžadovalo akutní lékařskou pomoc. Cílem je dosažení úplného duševního nebo fyzického zdraví u chronicky nemocných pacientů. [23]

3.1.3 Oddělení v nemocnicích

Tato kapitola charakterizuje vybraná nemocniční oddělení, která jsou důležitá pro zajištění akutní i dlouhodobé péče pro pacienta. Příklad možné organizační struktury jednotlivých oddělení je znázorněn na Obr. 1.

Anesteziologicko - resuscitační oddělení

Anesteziologicko - resuscitační oddělení neboli „ARO“ zajišťuje anesteziologickou a resuscitační péči a umožňuje provádět léčebné a operační výkony, dále vyšetřovací metody v regionální nebo celkové anestezii. Jedná se o přednemocniční a nemocniční péči o pacienty v kritickém stavu s ohrožením základních životních funkcí. Oddělení spolupracuje s operačními i neoperačními obory. [21]

Chirurgické oddělení

Toto oddělení poskytuje kompletní ambulantní a lůžkovou péči pro pacienty všech věkových kategorií a konziliární službu pro další oddělení nemocnice. Jsou zde prováděny operace v oblasti chirurgie břišní, cévní, dětské, hrudníku, prsu, plastické, septické apod. Jedná se o oddělení vybavené vyspělou technikou pro provádění životně důležitých i estetických operací, zajišťující maximální bezpečnost a benefity pro pacienta. [21]

Jednotka intenzivní péče

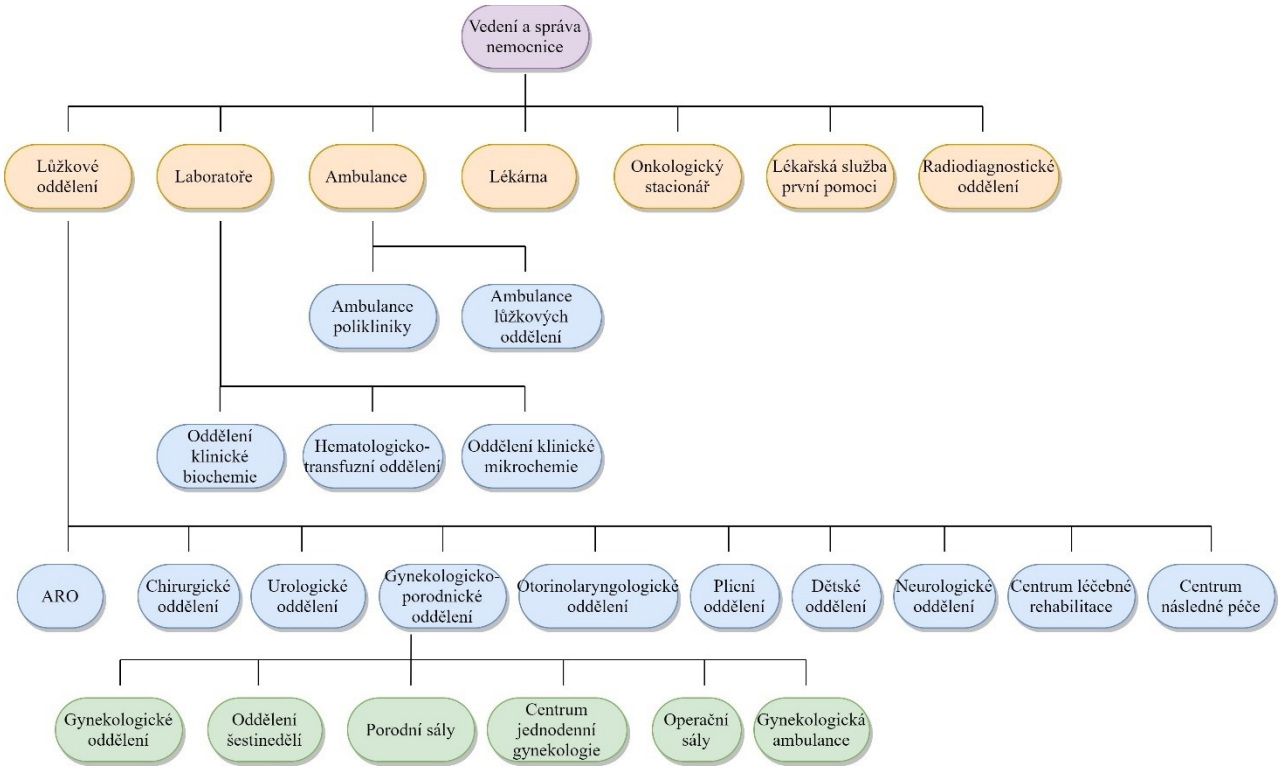
Toto oddělení, které je ve společnosti často nazýváno pouze zkratkou „JIP“, se zaměřuje na péči o dětské i dospělé pacienty, kteří vyžadují intenzivní péči, např. monitorování životních funkcí a zavedení intenzivní léčby. Oddělení bývá vybaveno nejmodernější medicínskou technologií umožňující monitoring a diagnostiku život ohrožujících stavů. [39]

Dětské oddělení

Dětské oddělení poskytují celkovou péči pro nezletilé, a to všech věkových kategorií. Některé nemocnice mají samostatně v rámci oddělení vybudovanou JIP, která umožňuje ošetřování závažných stavů dětských pacientů. [21]

Centrum následné péče

Centrum následné péče neboli „CNP“ je oddělení, které poskytuje následující zdravotnickou péči u pacientů, kteří nejsou v ohrožení života, ale jejich zdravotní stav neumožňuje propuštění do domácí péče nebo sociálního zařízení. [21]



Obr. 1 – Příklad organizační struktury oddělení v nemocnici [autor]

4 Bezpečnost nemocničních zařízení

Osoby, které se vyskytují v nemocničním prostředí, ať už se jedná o pacienty, zaměstnance, nebo návštěvníky, představují širokou škálu osobnostních skupin. Mohou se zde vyskytovat novorozenci, dospívající nebo lidé středního až pokročilého věku, zároveň každá z těchto osob vyžaduje jedinečné potřeby. Nezřídka se stává, že zdravotní stav omezuje pacienta v převzetí plné odpovědnosti za vlastní zajištění ochrany. Povinností nemocnic je proto zajistit pro přítomné osoby prostředí s přijatelnou mírou bezpečnosti. Tento závazek je především vyžadován, pokud pacient není schopen samostatné sebeobrany s ohledem na fyzické či psychické omezení. Jako příklad je možné uvést omezení z důvodu věku, demence, snížené mobility či jiným problémům duševního zdraví. Mnohdy bývá ohrožen také zdravotnický personál, který se denně setkává s lidmi, kteří bývají silně rozrušení kvůli ohrožení zdraví svého nebo svých blízkých. [47]

V souvislosti s ochranou nemocnic lze pojem bezpečnost obecně definovat jako stav zajišťující ochranu hmotného i nehmotného majetku a dosažení přijatelné míry bezpečnosti pro všechny osoby působící v rámci organizace a jejího prostředí, ať už se jedná o zaměstnance, pacienty, návštěvy, nebo dodavatele. Tato definice nepochybně neřeší problém s definováním relativní bezpečnosti, jelikož zabezpečení není statické, ale dynamické a lze jej považovat za stav, který se mění v čase. Jak se mění prostředí a lidské podmínky, mění se také stav nebo úroveň ochrany. Proto by každá organizace měla neustále přehodnocovat a následně modifikovat svůj zavedený systém ochrany. Je obtížné zhodnotit prostředí konkrétního zařízení tak, aby bylo možné určit, zda bylo ve skutečnosti relativní bezpečnosti dosaženo. Je to dáno tím, že tato hodnocení bývají do jisté míry subjektivní. Cílem implementace bezpečnostních opatření je snížit pravděpodobnost vzniku škodlivých incidentů a zamezit, nebo alespoň zmírnit újmu na chráněném zájmu, nikoli nutně eliminovat všechna uvažovaná rizika. [47]

Cílem bezpečnostní politiky každé nemocnice by měly být následující body: [36]

- napomáhat celkovému cíli zdravotnické organizace jakožto poskytování zdravotnických služeb;
- předcházet bezpečnostním incidentům prostřednictvím bezpečnostních opatření;
- reagovat na bezpečnostní incidenty tak, aby byly na co nejnižší možnou míru minimalizovány škody na chráněném zájmu;

- vytvářet pocit bezpečného prostředí v podvědomí zaměstnanců, pacientů, návštěvníků a dalších osob;
- poskytovat bezpečnostní služby a činnosti efektivním způsobem, který je v souladu s cílem a předpisy dané nemocnice.

V následujících podkapitolách bude stručně popsána definice fyzické bezpečnosti spolu s popisem jednotlivých odvětví. Dále zde budou popsány systémy technické ochrany, požární ochrany a další signalizační a komunikační systémy, které jsou dnes standardně využívány v areálech nemocnic.

4.1 Pojem bezpečnost obecně

Pojem bezpečnost ministerstvo vnitra definovalo jako „*stav, kdy jsou na efektivní míru omezeny hrozby pro objekt a jeho zájmy a tento objekt je k omezení stávajících i potenciálních hrozeb efektivně vybaven a ochoten při něm spolupracovat.*“ [1] Obecně poté můžeme bezpečnost definovat jako společností stanovenou schopnost systému zamezit tomu, aby riziko překročilo předem stanovenou mez.

Pokud budeme hledat definici pojmu bezpečnost v cizojazyčné literatuře, dojdeme k tomu, že zahraniční odborníci ve svých publikacích bezpečnost rozdělují na dvě oblasti zvané SECURITY a SAFETY. Obor security zajišťuje ochranu před zamýšlenou trestnou činností (do této oblasti můžeme zařadit fyzickou ostrahu, systémy technické ochrany apod.), zatímco obor safety zajišťuje předcházení vzniku náhodných nehod (do této oblasti bychom mohli zařadit bezpečnost a ochranu zdraví při práci nebo požární ochranu). [37]

Fyzickou bezpečnost můžeme definovat jakou souhrn technických, organizačních a režimových opatření, které souží k zajištění ochrany života a zdraví osob, životního prostředí a k zamezení neoprávněné manipulace s majetkem. Fyzickou bezpečnost tvoří:

- systémy technické ochrany (STO):
  - poplachové zabezpečovací a tísňové systémy;
  - dohledové videosystémy;
  - mechanické zábranné prostředky;
  - elektronické systémy kontroly vstupu;
- fyzická ostraha;

[1] SOUČEK, Vladimír, Eva STAŇOVÁ a Martin LINHART. *Vnitřní bezpečnost a veřejný pořádek: Krizové řízení* [online]. Praha, 2005, , 123 [cit. 2020-08-10]

- režimová ochrana.

Mimo STO se v dnešní době hojně využívají systémy elektrické požární signalizace (dále jen EPS). Přestože systémy EPS nejsou dle normativních a právních předpisů zařazeny mezi STO, slouží i tyto systémy k ochraně života a zdraví osob a také k minimalizaci následků při vzniku požáru.

Níže uvedené podkapitoly popisují systémy, služby a opatření spadající jak do kategorie SECURITY, tak do kategorie SAFETY.

4.2 Systémy technické ochrany v nemocničních zařízeních

Smyslem instalace STO je zabránění, znesnadnění, případně omezení nelegálního vstupu do areálu nebo objektu, zajištění spolehlivé a včasné detekce neoprávněného vstupu a pohybu ve střežených prostorách, evidence oprávněných vstupů a vjezdů do objektu a zajištění včasné signalizace poplachových stavů tak, aby byla zajištěna správná a včasná opatření v případě narušení objektu neoprávněnými osobami. V následujících podkapitolách budou popsány systémy technické a požární ochrany, které jsou typicky využívány pro zvýšení bezpečnosti v objektech nemocnic.

4.2.1 Mechanické zábranné prostředky

Mechanické zábranné prostředky (dále jen MZP) jsou základní a klasickou ochranou objektu a představují tzv. pilíř STO. MZP představují všechny kovové i nekovové prostředky, které spolu tvoří soubor mechanické ochrany objektů. Základní funkcí těchto prostředků je vytvoření pevné zábrany, která snižuje pravděpodobnost násilného vniknutí neoprávněných osob a tím zabraňuje znehodnocení, nebo v horším případě ke krádeži movitého či nemovitého majetku. Mezi ně můžeme zahrnout ploty včetně vrcholové zábrany a podhrabové překážky, brány, branky, závory, turnikety, okna, mříže, fólie a dveře včetně uzamykacího systému apod. [9]

Při návrhu MZP je nutné dbát na správnou volbu technického řešení a na požadovanou bezpečnostní třídu daného prvku, která splňuje klasifikaci dle NBÚ. Pyramida bezpečnosti je nástrojem pro provedení certifikace výrobků MZP, kdy se jedná o tzv. bezpečnostní třídu dle normy ČSN EN 1627. Klasifikace prvků do bezpečnostní třídy souvisí s časem a nářadím, které jsou potřeba na překonání MZP. Dle normy je

definováno celkem 6 bezpečnostních tříd, nicméně v ČR se můžeme setkat pouze s bezpečnostní třídou 1 až 4. ([27], [17])

4.2.2 Poplachové zabezpečovací a tísňové systémy

Poplachové zabezpečovací a tísňové systémy (dále jen PZTS) jsou využívány k ochraně majetku. Poplachový stav je signalizován (zpravidla opticky nebo akusticky) na určité místo, např. DPPC. Technické požadavky týkající se systémů PZTS upřesňují normy řady ČSN EN 50131. Systém se skládá z ústředny, která představuje jádro systému, expandérů (v jiných publikacích mohou být tyto prvky nazývány také koncentrátory nebo RIA), detektorů, signalizačních prvků, ovládacích prvků, přenosových zařízení, kabeláže apod. Přímo do systému je možné implementovat přístupové čtečky a elektromechanické zámky pro zamezení neoprávněného vstupu do střežených prostorů.

Systémy PZTS bývají rozděleny do pěti chráněných oblastí, a to:

- perimetrická ochrana;
- plášťová ochrana;
- prostorová ochrana;
- předmětová ochrana;
- tíseň.

Perimetrická ochrana:

Perimetrická ochrana (v jiných publikacích se můžeme setkat s pojmem obvodová ochrana) je ochrana, která slouží k detekci pachatele již na počátku páchání protiprávní činnosti. Jedná se o speciální aplikaci elektronických, elektromechanických a technických systémů, které se instalují na perimetr objektu.

Plášťová ochrana:

Plášťová ochrana zajišťuje detekci překonání pláště budovy (stěny, okna, dveře, nadsvětlíky apod.). Nejvyužívanějšími prvky jsou magnetické kontakty, detektory tříštění skla, poplachové fólie, vibrační (otřesové) detektory.

Prostorová ochrana:

Prostorová ochrana slouží k detekci pohybu pachatele již v chráněném objektu. Pomocí prostorových detektorů je možné detekovat směr pohybu případného pachatele. Nejvyužívanější prvky této úrovně ochrany jsou pasivní infračervené detektory (dále jen PIR), mikrovlnné a ultrazvukové detektory. V dnešní době jsou stále více využívány tzv. multisenzorové (v některých publikacích se můžeme setkat s pojmem duální detektory), které kombinují dva a více principů detekce. Jako příklad můžeme uvést propojení PIR detektoru s mikrovlnným detektorem. Tato kombinace zajišťuje snížení planých poplachů na základě logické provázanosti obou detekčních principů.

Předmětová ochrana:

Předmětová ochrana se zaměřuje na ochranu konkrétních předmětů, jako jsou trezory, obrazy, vázy a další předměty, které představují pro majitele určitou hodnotu. Ve většině případů jsou tyto detektory programově přiřazené do samotných skupin, což umožňuje ponechat tyto detektory aktivní i v případě zvýšeného provozu.

Tíseň:

Tísňové hlásiče jsou magnetické kontakty nebo mikrospínače, jež jsou zapouzdřeny do podoby tlačítka malých rozměrů. Jsou určeny pro vyhlášení tísňového signálu v případě ohrožení. Hlásiče mohou vyhlašovat buď asistenci, nebo přivolání pomoci. Mohou být instalovány pevně (např. na pracovním stole), nebo se také využívají v mobilním (bezdrátovém) provedení, kdy je osoby nosí neustále při sobě. Nevýhodou tísňových hlásičů je absence ochrany před nechtěnou aktivací. [5]

4.2.3 Dohledové videosystémy

Dohledové videosystémy (dále jen VSS) umožňují monitorování, popřípadě pořizování záznamu prostorů v chráněném objektu a jejich zobrazování operátorovi. Problematiku systému VSS popisují normativní předpisy řady ČSN EN 62676. Systémy VSS slouží především jako preventivní ochrana před protiprávním jednáním a jako prostředek pro usvědčení potenciálního pachatele.

Dnešní trh nabízí dva druhy kamerových systémů, a to analogové a IP systémy. Starší typ analogového systému VSS přenáší signál z kamer v analogové formě obvykle za

pomoci koaxiální kabeláže, kdy kamera funguje jako konvertor obrazových dat. Výhodou analogových systémů jsou nižší pořizovací náklady, jednodušší nastavení kamer, nižší nároky na uložiště dat a nízká latence. Bohužel tyto „zastaralé“ systémy mají i výrazná omezení. Největším omezením je nižší kvalita obrazu, kdy tento typ neumožňuje pořizovat obrazový záznam takové kvality jako IP systémy. Omezená velikost maximálního rozlišení neumožňuje zajišťovat tzv. identifikaci osob. Další nevýhodou je poté nákladnější kabeláž, kdy jednotlivé kamery je potřeba napájet samostatným kabelem, v případě otočných kamer je potřeba dalšího sběrnicového kabelu pro jejich ovládání. Část nevýhod analogových kamer řeší systémy HDCVI, které umožňují digitální přenos dat o rozlišení až 1080p po koaxiálním kabelu. Nicméně převážná většina dnešních instalací využívá tzv. IP kamery. Tyto kamery tvoří digitalizovaný videosignál, který se přenáší prostřednictvím počítačových sítí, což umožňuje přenášet větší množství datového toku. Jednou z největších předností IP kamerových systémů je vysoké rozlišení, přenos signálu bez ztráty kvality na libovolnou vzdálenost a využívaní tzv. videoanalytických funkcí. Mezi zmíněné funkce patří např. detekce obličeje, detekce opuštění/přidání objektu, narušení zóny, překročení zóny, změna scény, počítání osob, detekce požáru apod. Narůstající výkon dnešních kamer umožňuje provádět pokročilejší analýzy přímo v kameře, a to bez záznamového zařízení. Dnešní systémy jsou často vybaveny umělou inteligencí (AI), která umožnila zajistit výrazný pokrok ve vývoji videoanalytických funkcí. Další výhodou IP systémů je provedení kabeláže, kdy se pro napájení a datový přenos z kamery využívají PoE, popř. PoE+ porty. Ty umožňují napájení a přenos dat prostřednictvím jediného ethernetového kabelu. [16]

Dohledové videosystémy zahrnují velkou část bezpečnostního plánování ve zdravotnictví. Díky schopnostem systému sahajícím od jednoduchého dohledu až po využití videoanalytických funkcí, řízení přístupu, správu návštěvníků, nouzovou správu nebo dokonce i zlepšování péče o pacienty, pomáhají moderní videosystémy zdravotnickým zařízením splňovat složité požadavky na zvyšování bezpečnosti. [44]

4.2.4 Elektronické systémy kontroly vstupu

Systémy ESKV nabízejí v objektech, kde se vyskytuje zvýšený pohyb osob, široké možnosti řízení vstupů a průchodů pomocí přidělených oprávnění na základě autorizace. Dále umožňuje zajišťování evidence a reportingu, včetně spouštění navazujících akcí. Správně nastavený systém umožňuje vstup do objektu pouze osobám, které mají práva ke vstupu do uzavřeného prostoru. Systém po identifikaci uživatele může odemknout či odkódovat související prostory v objektu, nebo spustit navazující technologie. Jelikož systémy ESKV umožňují automatizované řízení vstupu, majitel nebo provozovatel objektu má přehled o příchodech a odchodech jednotlivých osob, popřípadě dostává informaci ohledně počtu osob v objektu. Kontrola vstupu může fungovat na perimetru a plášti objektu, na vstupech do určených zón objektu nebo na vstupu do režimových pracovišť. ([27], [19])

Na trhu se vyskytují dva druhy systémů, a to autonomní a síťové. Autonomní systémy mají malou schopnost komunikace, proto jsou programovány přímo u dveří, které ovládají. Problémem takového systému je především složitější správa, pokud ovládá vyšší počet dveří. Naopak výhodou tohoto typu je cena a nižší požadavky na kabeláž. U síťového druhu systému ESKV komunikují všechny vstupy s centrálním prvkem, čímž je umožněno centrálně monitorovat a ovládat vstupy do prostorů z jednoho místa. [19]

Identifikace osoby může probíhat prostřednictvím přístupových kódů, bezkontaktních karet, čteček nebo sejmutím biometrického údaje. Využití přístupových kódů není z hlediska bezpečnosti nejlepší volba, jelikož potenciální pachatel může získat přístupový kód nebo jej vysledovat z pohybu ruky. Využití ID karet je sofistikovanější možností, ale nebezpečí spočívá v jejím odcizení nebo ztrátě. Proto nejvýhodnější možností je bezesporu využití biometriky. Nejpřesnější a nejvyužívanější metoda je snímání oční duhovky. [19]

4.2.5 Integrační nadstavbový software

Integrační nadstavbový software umožňuje centralizovaně řešit ovládání a vizualizaci sytému technické a požární ochrany a usnadňuje dohled nad stavem instalovaných systémů v rámci jedné přehledné platformy. Do softwaru je možné integrovat systémy PZTS, EPS, ESKV, VSS a mnohé další. Nadstavbový systém poté umožňuje uživateli poskytovat rozsáhlé nástroje jako: [7]

- monitoring a vizualizace objektu;
- jednotný přehled o událostech;
- jednotné ovládání;
- centrální správu jednotlivých systémů;
- automatizaci;
- analýzu a vyhodnocování informací;
- centrální správa uživatelů;
- synchronizace času napříč systémy;
- podpora krizové managementu.

Do softwaru je potřeba implementovat jednotlivé mapové podklady objektů, například v podobě vhodných dispozičních výkresů. Do těchto výkresů jsou poté vyznačeny jednotlivé ikony znázorňující jednotlivé detektory nebo hlásiče bezpečnostních systémů. Obsluha je následně schopna sledovat stavy jednotlivých komponentů, v případě poplachu je obsluha akusticky upozorněna. Daný prvek je v případě poplachu zvýrazněn. V případě, že je v nadstavbovém systému implementován také VSS, může obsluha místo ověřit vizuálně za pomoci přítomné kamery. [7]

4.3 Fyzická ostraha

Fyzická ostraha (dále jen FOs) představuje nejstarší, nejvyužívanější, ale také finančně nejnáročnější formu ochrany osob a majetku. Jedná se o soubor činností fyzické osoby, která je odborně způsobilá, jejímž hlavním úkolem je zajišťovat ochranu osob a majetku, bezpečnost objektů a veřejný pořádek. Cílem této činnosti je snížení pravděpodobnosti vzniku protiprávního jednání. FOs může být zajišťována: [15]

- komerční bezpečnostní službou;
- vlastními vyškolenými zaměstnanci organizace a podniků;
- státní ochrannou službou (ojedinělé případy).

Hlavními úkoly FOs jsou ochrana a ostraha movitého a nemovitého majetku na místech veřejně přístupných či nepřístupných, ochrana osob, zajišťování výjezdových zásahových služeb při připojení objektu na dohledové poplachové a přijímací centrum, zajišťování pořádku na veřejných místech, zabraňování neoprávněného vstupu osob či vozidel do střeženého objektu, podílí se na obsluze STO apod. Pracovníci FOs mohou také

plnit informační roli na vrátnicích, řešit mimořádné události a nestandartní bezpečnostní situace a v neposlední řadě plní roli prevence před protiprávním jednáním. [15]

FOs je často považována za základní pilíř bezpečnostní politiky v nemocničních zařízeních. Pracovníci ostrahy patří mezi první osoby, se kterými se pacienti a návštěvníci při vstupu do nemocnice střetnou, popřípadě s nimi komunikují. Tyto osoby by měly zvyšovat celkovou úroveň bezpečnosti objektu a přispívat pocitu bezpečnosti u veřejnosti. Proto bezpečnostní politika nemocničních zařízení potřebuje spolehlivé a profesionální bezpečnostní pracovníky. [47]

V nemocničních zařízeních může být FOs zajišťována několika způsoby. Některé nemocnice nemají žádný vyhrazený bezpečnostní personál a místo toho se spoléhají pouze na výjezdové skupiny bezpečnostních pracovníků, kdy je objekt připojen na dohledové poplachové a přijímací centrum (ve zkratce DPPC). Některé organizace se rozhodnou svěřit své bezpečnostní úkony externímu dodavateli, zatímco jiné mají kombinaci vlastního i smluvního bezpečnostního personálu. Stále existuje část zařízení, které se spoléhají pouze na svůj vyškolený personál. [28] Pokud si organizace zajišťuje FOs z vlastních řad personálu, jedná se sice z ekonomického hlediska o příznivou variantu, ale z hlediska profesionality není tato forma optimální, jelikož tito zaměstnanci nebývají dostatečně vyškoleni a seznámeni s rozsahem a postupem jejich práce v souladu s platnými právními předpisy. Tímto se pak FOs stává jedním z nejslabších článků celé fyzické bezpečnosti organizace.

4.4 Režimová ochrana

Jedná se o ucelený soubor administrativních a organizačních opatření, a to zejména opatření, zákazy, příkazy, pokyny, omezení, která jsou stanovena dokumenty a řídícími předpisy dotčeného objektu. Cílem režimových opatření je stanovit pravidla pro správné využívání bezpečnostních opatření a zajistit vazby mezi uživateli objektu a prvky fyzické bezpečnosti. Jedná se o zákazy, omezení, příkazy, stanovení režimů, psaná či domluvená pravidla pro pohyb vozidel a osob do a z objektu, jejich pohyb v objektu, pokyny pro manipulaci s materiálem, pokyny pro nakládání s citlivými informacemi, činnost fyzické ostrahy, postupy pro řešení nestandardních bezpečnostních situací apod. Mezi režimová a organizační opatření patří tzv. bezpečnostní zónování, kdy je objekt rozdělován do několika zón. Mezi ně patří vnější zóna, zóna zaměstnanců, zóna pacientů, zóna návštěv,

interní zóna a interní chráněná zóna. Tyto zóny musí mít jasně definované hranice a pravidla pro vstup či pohyb. ([15], [31])

Pro správnou funkčnost celé bezpečnostní politiky nemocnic je nezbytné zajistit důležité interní předpisy a úkony. Jedná se například o organizační a provozní řády, návštěvní řády, směrnice, zajištění školení zaměstnanců zaměřené na dodržování organizačních a režimových opatření, zajišťovat bezpečnostní audity apod. Režimová opatření splňují svůj význam, pokud projdou všemi úrovněmi zaměstnanců a pokud je jejich realizace úplná, kvalitní a kvalifikovaná. [12]

Podstatným úkonem při zřizování a provozu STO je správa instalovaných technologií a zajištění správy instalovaných odpovědnou osobou. Jelikož není ve všech organizacích tato problematika řešena, následkem může být bezpečnostní systém, který není vhodně nastaven. Režimová a organizační opatření by také měla být dostatečně provázána s instalovanými systémy technické a požární ochrany.

4.5 Elektrická požární signalizace

Elektrická požární signalizace (dále jen EPS) je systém patřící dle vyhlášky č. 246/2001 Sb., o požární prevenci mezi vyhrazené požárně bezpečnostní zařízení (dále také PBZ). Systém EPS zajišťuje včasnou lokalizaci ohniska nebo detekci již vzniklého požáru a předání informace o požáru oprávněným osobám. Systém se skládá z jedné nebo více ústředen, hlásičů, ovládacích, signalizačních a přenosových zařízení, napájecích zdrojů apod. Pomocí vstupně/výstupních prvků systém EPS umožňuje ovládat další zařízení nebo celé systémy, které zabraňují dalšímu šíření požáru, či usnadňují protipožární zásah.

4.6 Evakuační rozhlas

Systém evakuačního rozhlasu je obvykle instalován do veřejných prostorů, kde se vyskytuje velký počet osob, jako jsou nemocnice, metra, letiště, nákupní centra apod. Cílem instalace systému je za pomoci hlasové zprávy informovat přítomné osoby o zjištěném nebezpečí, čímž dochází ke snížení pravděpodobnosti vzniku paniky a chaosu. Dle zjištěných informací osoby dokáží reagovat na hlasovou zprávu o nouzové situaci efektivněji než na zvukový tón, proto jsou tyto systémy dnešní době důležitou částí bezpečnostního managementu objektů. Hlasová zpráva informuje osoby v objektu o tom,

co dělat v případě vzniku mimořádné situace a tím efektivně řídit evakuační proces. Evakuační rozhlasy jsou propojovány s dalšími systémy technické a požární ochrany, nicméně je lze v případě normálního stavu využívat např. na reklamní sdělení či hudební a rádiové podkresy nebo paging. Pokud je indikován poplach, systém ihned vyřadí všechny funkce, které nejsou spojeny s funkcí nouzového systému. [11]

Úspěšná evakuace je závislá na spolehlivosti, výkonu a srozumitelnosti systému hlasového poplachu, a proto nejdůležitějšími parametry jsou kvalita použitých prvků, kabelová instalace, která musí být vyrobena z materiálů odolných vůči vysokým teplotám, aby byl zajištěn trvalý provoz systému i v případě požáru. Jednotlivé požadavky jako minimální a maximální akustický tlak, hladinu hlasitosti nad úroveň zvuku, srozumitelnost a další udává norma ČSN EN 50849. [48]

4.7 Vnitřní komunikační systémy

Tyto systémy nespadají přímo do kategorie STO, nicméně mohou být využívány k zajištění komunikace pro předávání informace o poplachu na předem vytipovaná místa. Běžně se jedná o klasické telefonní systémy zajišťující vnitřní komunikaci mezi zaměstnanci jednotlivých oddělení. Každý zaměstnanec je vybaven komunikačním prvkem, například telefonem, kterému je přiřazena unikátní číselná klapka.

4.8 Systém sestra – pacient

Jedná se o dorozumívací a signalizační zařízení, které je určené pro využití v objektech nemocnic, domovech důchodců, hotelech, lázeňských domech apod. Systém se používá s kombinací hlasové služby k přivolání pomoci, ať už té lékařské, nebo pomoc v případě napadení. Systém následně zajišťuje akustickou signalizaci u hlavního terminálu v místech s přítomností personálu a optickou signalizaci v pokojích a na chodbě nad vstupem do dané místnosti. Zařízení lze propojovat s telefonní ústřednou, tlačítky a táhly nouzového volání, které jsou umístěny na sociálních zařízeních nebo chodbách. Systém může ovládat nespočet elektromechanických zámků, může fungovat jako evakuační rozhlas, popřípadě být propojen např. s dohledovým videosystémem. Na dispečerském stanovišti lze poté kontrolovat, kdo právě volá, ze kterého telefonního čísla, čísla pokoje nebo jména pacienta. ([10], [20])

5 Posouzení rizik nemocnic

Jak zmiňuje úvod diplomové práce, pocit bezpečí patří mezi základní lidské potřeby a prioritně se odvíjí od stavu, v němž se člověk nachází. Na potřebu bezpečí a jistoty poukazuje tzv. Maslowova pyramida, která tuto potřebu zařazuje na druhou příčku.

Pojem riziko lze popsat hned několika definicemi. První možnou definicí je, že riziko představuje pravděpodobnost vzniku události spolu se vznikem nějaké ztráty. Další definice popisuje riziko jako událost, která může negativně ovlivnit funkčnost např. námi posuzovaného zdravotnického zařízení a tato událost má určitou pravděpodobnost a důsledky. V rámci zdravotnických zařízení je pojem riziko úzce spojován s globálním úsilím zajistit bezpečnost ošetřovatelské a léčebné péče. [38]

Prostředí zdravotnických zařízení představuje samo o sobě určité riziko. Všeobecně je známo, že se násilí ve větší míře vyskytuje na pracovištích, kde je součástí profese práce s lidmi. Zaměstnanci se zde setkávají s lidmi, kteří jsou ve stresu a těžké životní situaci z důvodu zhoršení zdravotního stavu svého nebo svých blízkých. Dále se v nemocnicích často pohybují lidé trpící duševní nemocí, zažívající psychické trauma nebo jsou pod vlivem omamných látek. Nicméně také pacienti nebo návštěvníci se mohou stát obětmi výhružek a útoků, jelikož zdravotnický personál často pracuje pod velkým tlakem a nad rámec svých možností, což může v zaměstnancích vyvolávat zvýšenou agresivitu. [51] Zvýšená agresivita a vznik násilí může souviset například s:

- psychickým napětím pacientů;
- nedostatečným zajištěním bezpečného prostředí;
- vysokým pracovním vytížením zaměstnanců;
- prací s rizikovou skupinou osob;
- způsobem zacházení s pacienty během pracovních úkonů;
- dlouhými frontami na lékařských pracovištích.

Pokud bychom se podívali na aktuální situaci ve světě, měli bychom se zaměřit i na celosvětovou pandemii virové choroby COVID-19, jelikož aktuální řešení pandemické situace rozděluje společnost na dvě strany. Jedna strana společnosti má z následků pandemie obavy a je ochotna dodržovat veškerá vládní a hygienická opatření. Druhá strana se dívá na nařízená opatření negativním pohledem, ohrazuje se proti omezování jejich svobody a zastává názor, že virová choroba nemá takové dopady na naši společnost, jak je medializováno. Tyto názory mohou při nařizování dalších opatření vyvolávat ve

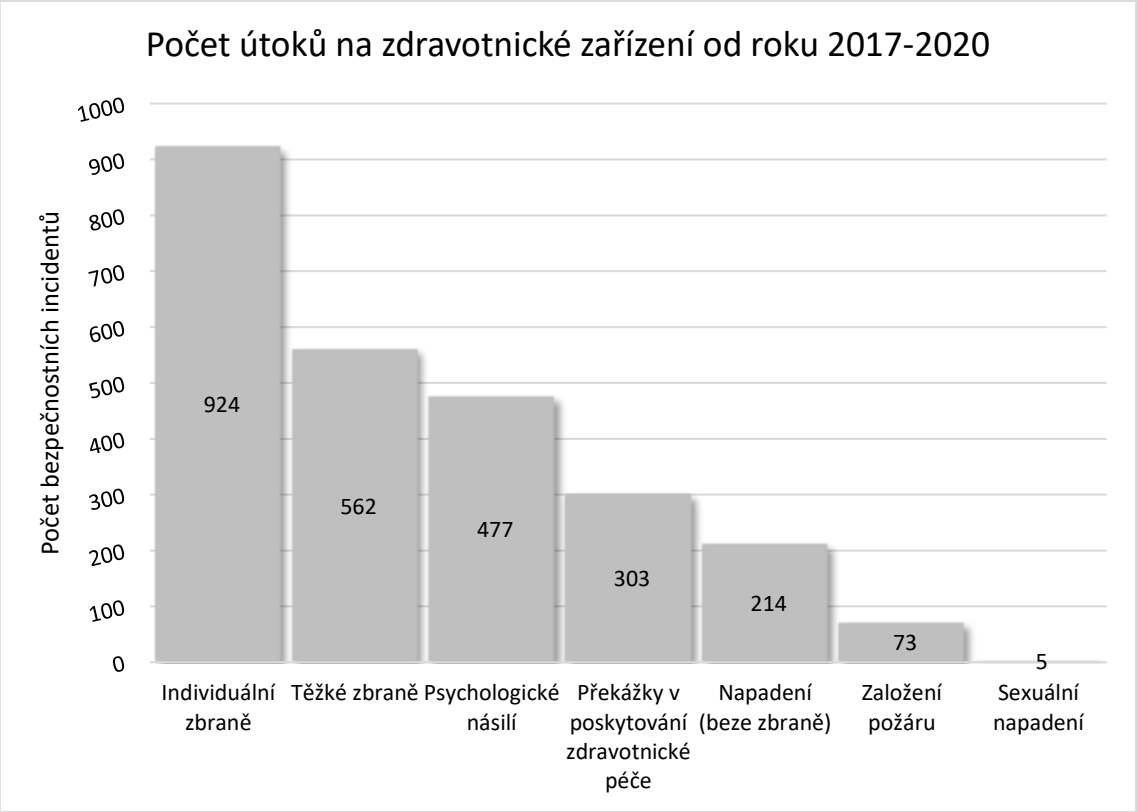
společnosti nepokoje a násilí, což se může odrazit na zvyšování počtu útoků v nemocnicích. Útoky by mohly mít nejen přímý dopad na schopnost zdravotnického systémů vykonávat své služby, ale mohou mít dopad na psychosociální zdraví pacientů a poskytovatelů zdravotní péče. [3]

Z hlediska cílených útoků na nemocnice by neměly být opomenuty teroristické útoky. Jejich nedávný vývoj ve světě naznačuje, že se útoky mohou vyskytnout v podstatě kdekoli a kdykoli. Nový model terorismu se zaměřuje spíše na větší počet osob než na jednotlivce. Na území České republiky se teroristické útoky na nemocniční zařízení téměř nevyskytují. Nicméně je potřeba, aby bezpečnostní politika těchto zařízení byla připravena na případný útok tak, aby v nejlepším případě útoku zabránila, nebo alespoň snížila dopad na chráněné zájmy.

5.1 Průzkum bezpečnostních incidentů ve světě

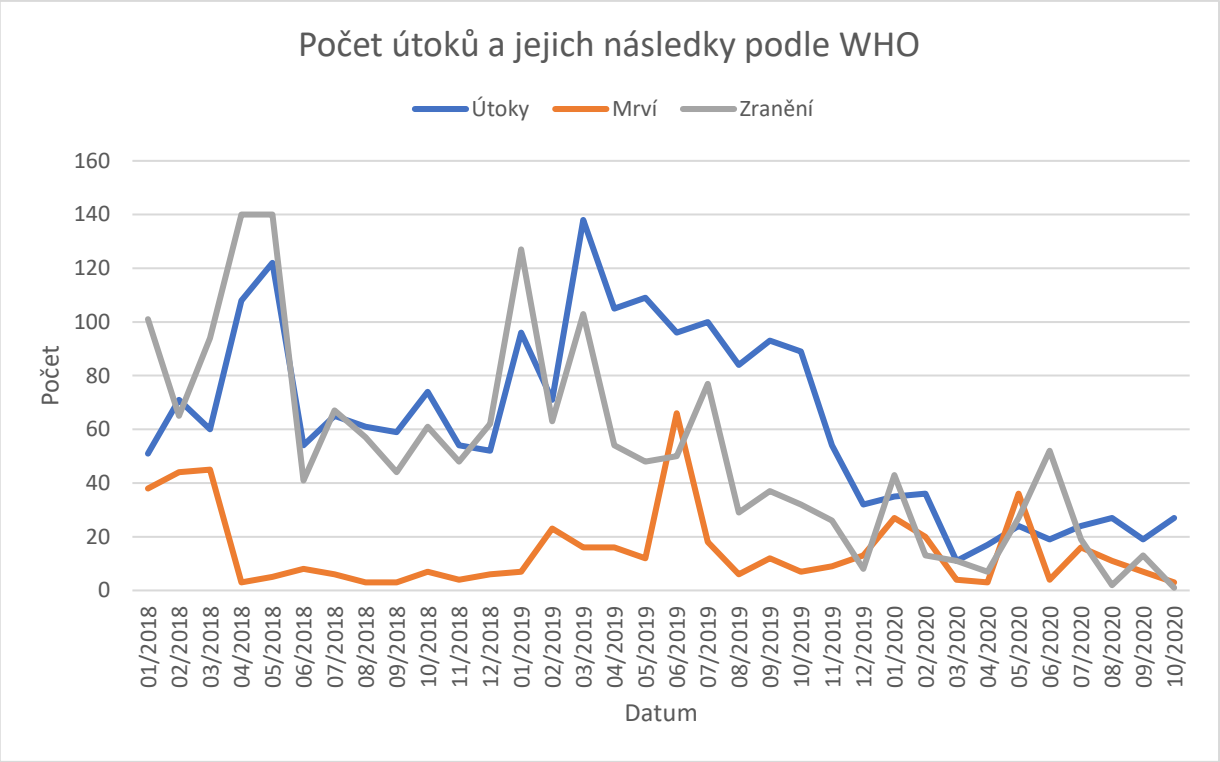
V průběhu několika let došlo na území ČR, ale i v ostatních státech Evropské unie, k několika útokům ve zdravotnických zařízeních, při nichž zemřelo několik osob. WHO definuje útok na zdravotnická zařízení jako jakýkoli akt představující verbální nebo fyzické napadení, které narušuje dostupnost poskytování léčebných nebo preventivních zdravotnických služeb [34].

Od roku 2017 WHO zprostředkovává databázi útoků na zdravotnická zařízení, kterou nazývá Dohledový systém útoků na zdravotnictví. Dle této databáze došlo za poslední 3 roky celkem k 1967 útokům, přičemž většina údajů jsou ze států severní Afriky. Přibližně 65 % útoků mělo dopad na životech a zdraví zdravotnického personálu, okolo 31 % útoků mělo dopad na objekty zdravotnických zařízení, celkem 23 % útoků mělo dopad na dopravní prostředky zdravotnické péče, zhruba 14 % útoků mělo dopad na zdravotnické vybavení a 8 % útoků mělo dopad na životech a zdraví pacientů. Vytvořený Graf 1 prezentuje počty bezpečnostních incidentů ve zdravotnických zařízeních dle statistik WHO. [36]



Graf 1 – Počet útoků na zdravotnická zařízení [autor, data z [24]]

Na základě Graf 1 je možné konstatovat, že největší procentuální zastoupení mají útoky individuální zbraní (WHO zde zařazuje např. o nůž, pistol, granát, amatérsky vyrobené nástražné výbušné systémy apod.). Druhou pozici zaujímají útoky těžkými zbraněmi (pro jejich využití je dle WHO potřeba více než jedné osoby a jedná se např. o minomety, bombardéry, tanky, střelné zbraně apod.). Poté následuje psychologické násilí (vyhrožování či zastrašování) a překážky v poskytování zdravotnické péče. Pátým nejzastoupenějším druhem útoku je fyzické napadení beze zbraně (fyzické, administrativní nebo právní). Dalšími typy útoku jsou také žhářské útoky nebo sexuální napadení. Graf 2 znázorňuje údaje o počtech útoků a jejich následných dopadech. Dle WHO došlo od prosince roku 2017 do října roku 2020 celkem k 1 976 útokům na zdravotnická zařízení v celkem 16 zemích (především státy severní Afriky), při kterých bylo zraněno celkem 1 697 lidí a 463 lidí bylo usmrceno.



Graf 2 – Počet útoků a jejich následky dle WHO [autor, data z [24]]

Cizojazyčný výzkum *Occupational Medicine* [25] naznačuje, že počty verbálních a fyzických útoků na zdravotnický personál narůstají. Výzkum byl proveden v několika zemích Evropské unie. Z celkového počtu dotazníků bylo relevantních pouze necelých 40 000 dotazníků, což představovalo cca 51 % dotazníků. Výsledky výzkumu jsou přepsány do tabulky, která je součástí Přílohy č. 2. Hodnoty v tabulce ukazují, že se celkově s napadením setkalo přibližně 22 % zdravotních sester na různých pozicích.

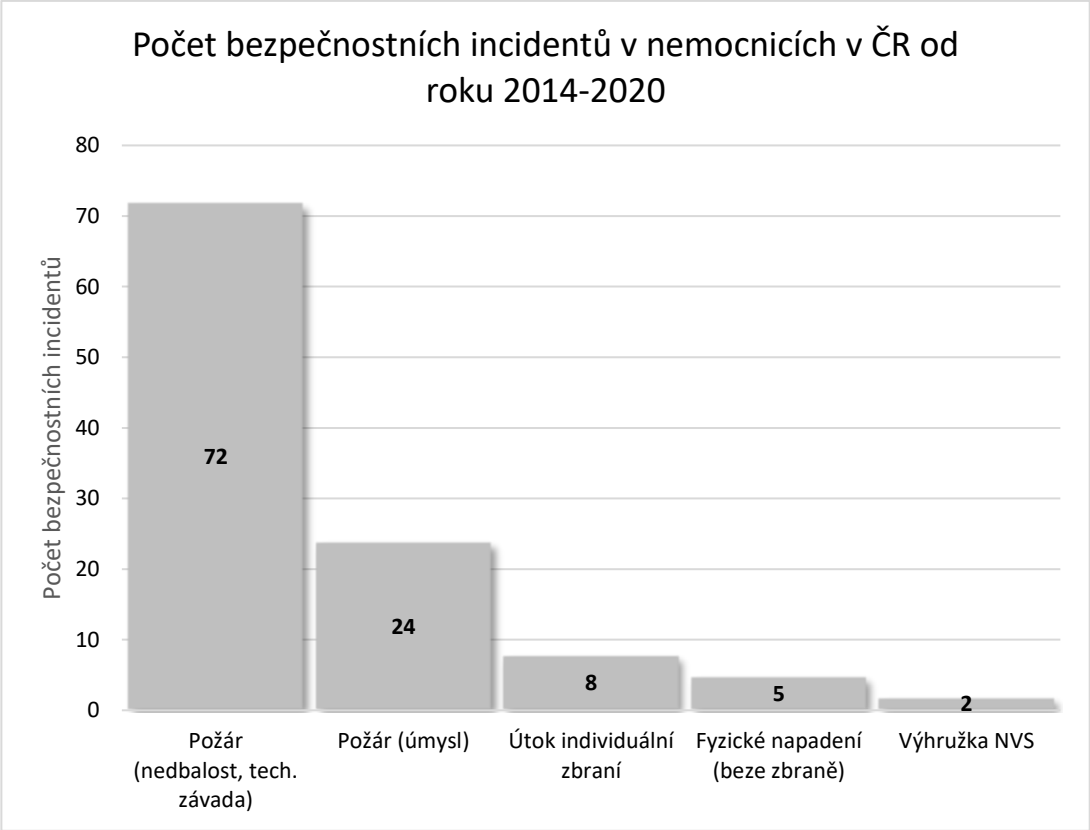
Další studií zabývající se násilím mířeným proti zdravotním sestrám ve vybraných evropských zemích je studie „*Reporting of workplace violence towards nurses in 5 European countries – a cross-sectional study*“ [4]. Ve studii bylo osloveno celkem 1089 respondentů profese zdravotní sestra při následujícím zastoupení ve smyslu jednotlivých států (Polsko – 265; Česká republika – 324, Slovenská republika – 200; Turecko – 200 a Španělsko – 100). Celkem 69 % účastníků studie uvedlo, že se s násilím a agresivitou na pracovišti setkali. Významné procento představující zkušenost s násilím na pracovišti zaujímaly české zdravotní sestry (88 %). Pro srovnání např. na Slovensku se potýkalo s násilím 32 % sester. Výsledky studie také naznačovaly, že pouze 23 % sester vědělo, jak v takové situaci postupovat. Na stupnici od 1 do 5 (1 – „*nemám obavy*“; 5 – „*velmi se*

obávám“) respondenti odpovídali, do jaké míry mají z násilí na pracovišti obavy. Dle výsledků mají největší obavy sestry na psychiatrických, pohotovostních a ambulantních odděleních. Nejběžnější formou násilí byly verbální útoky. Za poslední rok čelilo této formě celkem 54 % respondentů. Větší část z nich uvedla, že danému incidentu nebylo možné nijak předejít. Celkem 20 % respondentů také uvedlo, že se za poslední rok potýkalo také s fyzickým útokem. Jednalo se zejména o respondenty pracující na psychiatrických odděleních, v hospicích, domovech pro seniory a rehabilitačních centrech. [4]

5.2 Průzkum bezpečnostních incidentů v České republice

Dle provedeného průzkumu internetových zdrojů bylo zjištěno, že na území České republiky v období od roku 2014 do roku 2020 došlo v nemocnicích k několika bezpečnostním incidentům (viz Graf 3). Největší procento zastoupení zaujímají požáry, ke kterým došlo z důvodu nedbalosti, technické závady nebo samovznícení. Dalším častým bezpečnostním incidentem byly úmyslné požáry, tzv. žhářské útoky[2]. Následující pozici zaujímají útoky s využitím individuálních zbraní. Individuální zbraň může být např. nůž, střelná zbraň apod. Dále lze mezi časté bezpečnostní incidenty zařadit verbální a fyzické útoky neozbrojeným útočníkem. Většina těchto útoků začíná slovními výhružkami a v některých případech může končit právě fyzickým napadením. Nicméně tento typ útoku se v žádných statistikách neeviduje. Tyto případy bývají nejčastěji řešeny interně fyzickou ostrahou nemocnice, která většinu těchto incidentů řeší pouze vyvedením neukázněné osoby z objektu. Přesto lze předpokládat, že pokud by byl znám celkový počet těchto útoků, byl by zastoupen nejčastěji. Posledním typem útoků, který se za posledních šest let v ČR několikrát objevil, je vyhrožování nástražnými výbušnými systémy (dále jen NVS). Celkový přehled bezpečnostních incidentů v nemocničních zařízeních v ČR je uveden v Příloze č. 3.

[2] Statistické údaje o požárech z roku 2014 až 2019 poskytl pro účely zpracování diplomové práce pplk. Ing. Pavel Lukeš z generálního ředitelství HZS kraje.



Graf 3 – Počet bezpečnostních incidentů v nemocničních zařízeních v ČR [autor]

Ve článku „*Prevence násilí v ošetřovatelství v České republice*“ [29], který vydala společnost Journal of Nursing and Care v roce 2017, je provedena studie prostřednictvím dotazníků týkajících se násilí v ošetřovatelství. Výsledky výzkumu ukázaly, že početnější zastoupení zaujímají verbální útoky na ženy a zdravotní sestry. Nejvíce se s fyzickým útokem setkávají členové FOs. Výsledky výzkumu jsou uvedeny v Tab. 1.

Tab. 1 – Respondenti čelící verbálnímu a fyzickému napadení [29]

Napadení	Verbální	71,5 %
	Fyzické	18,5 %
	Žádné	10 %
Muži	Verbální	53,2 %
	Fyzické	36,2 %
Ženy	Verbální	76,4 %
	Fyzické	13,4 %
Zdravotní sestry	Verbální	77,2 %
	Fyzické	25,2 %
Lékaři	Verbální	65,2 %
	Fyzické	7,6 %
Záchranáři	Verbální	70,9 %
	Fyzické	25,2 %
Fyzioterapeuti	Verbální	66,7 %
	Fyzické	3,3 %
Členové FOs	Verbální	44,4 %
	Fyzické	56,6 %

5.3 Identifikace rizik

Proces identifikace rizik je založen na shromažďování rizik, včetně jejich zdrojů vzniku, které mohou vzniknout vně i uvnitř posuzovaného zařízení, a to na základě jejich nebezpečných vlastností. V rámci procesu identifikace musí být brána v úvahu také nebezpečí a jejich zdroje, která nejsou z hlediska závažnosti příliš závažná.

Pro identifikaci rizik je v první řadě vhodné definovat všechna aktiva, která se v areálech nemocnic nacházejí a mají být před riziky chráněna. Tato diplomová práce se zabývá pouze hmotnými aktivy spadajícími do kategorie ochrany životů a zdraví osob. Do této zvolené skupiny je možné zařadit následující aktiva:

- životy a zdraví zaměstnanců nemocnice;
- životy a zdraví pacientů;
- životy a zdraví návštěvníků a zákazníků (např. lékárny);

- životy a zdraví nájemníků;
- životy a zdraví dodavatelů.

V níže uvedené Tab. 2 jsou sepsána hlavní rizika, která mohou v nemocničních zařízeních vzniknout. Tabulka vychází zejména z metodiky s názvem „*Vyhodnocení ohroženosti měkkého cíle*“ [18], která se využívá pro rozhodování o rozvoji bezpečnostního systému vybraného měkkého cíle.

Tab. 2 – Identifikace rizik v nemocnici [autor, upraveno z [18], [13]]

Č.	Rizika
1	Vandalismus
2	Krádež
3	Vloupání
4	Verbální napadení
5	Fyzické napadení (beze zbraně)
6	Výhružka chladnou zbraní
7	Napadení chladnou zbraní s cílem ohrozit jednu vybranou osobu
8	Napadení chladnou zbraní s cílem ohrozit velký počet osob
9	Požár – technická závada/nedbalost
10	Žhářský útok s cílem ohrozit jednu vybranou osobu
11	Žhářský útok s cílem usmrtit velký počet osob
12	Použití zápalné láhve
13	Aktivní střelec
14	Útok střelnou zbraní s cílem ohrozit jednu vybranou osobu
15	Útok střelnou zbraní s cílem ohrozit velký počet osob
16	Nájezd atentátníka automobilem do objektu
17	Výhružka útoku s NVS
18	Sebevražedný útok s použitím NVS
19	Použití NVS s cílem usmrtit velký počet osob
20	NVS v zaparkovaném voze
21	Umístění NVS u zásobníku kyslíku
22	Umístění NVS u zdroje tepla nebo el. energie
23	Použití nebezpečné biologické látky

V Příloze č. 4 je vytvořen Ishikawův diagram příčin a následků zpracovaný pro nemocniční zařízení, kde jsou sepsány možné příčiny vzniku bezpečnostních rizik.

5.4 Analýza rizik

Provedená analýza rizik poskytuje zpracovateli základní podklady pro rozhodnutí, zda je riziko přijatelné, či nikoli. Bere v úvahu zdroje a příčiny hrozeb, následky a pravděpodobnost výskytu. Samotné stanovení pravděpodobnosti výskytu vychází ze třech proměnných, které jsou charakterizovány jako dostupnost prostředků (D), výskyt (V) a složitost provedení (S) daného způsobu útoku. Jelikož se tato diplomová práce nezabývá konkrétním objektem, je před zpracováváním analýzy nutné podotknout, že úrovně jednotlivých proměnných jsou stanoveny pouze v obecné rovině. Hodnoty byly určovány dle doporučení již výše uvedené metodiky (viz [18]). Jednotlivé pravděpodobnosti jsou hodnoceny kvalifikovaným odhadem na škále od 1 do 7. Bodovací škály jsou uvedeny v tabulkách v Příloze č. 5. V Tab. 3 jsou stanoveny pravděpodobnosti proměnných D, V a S. Tyto pravděpodobnosti byly následně použity ke stanovení celkové pravděpodobnosti vzniku vybraných rizik. Celková pravděpodobnost rizik je následně vypočtena na základě vzorce č. 1.

$$P = D + V + S \qquad (1)$$

kde:

D – dostupnost prostředků;

V – výskyt daného způsobu útoku;

S – úroveň složitosti provedení.

Tab. 3 – Analýza pravděpodobnosti vzniku rizika [autor]

Č.	Riziko	Pravděpodobnost			Celková pravděpodobnost (P)
		Dostupnost (D)	Výskyt (V)	Složitost (S)	
1	Vandalismus	7	7	7	**21**
2	Krádež	7	7	7	**21**
3	Vloupání	7	6	7	**20**
4	Verbální napadení	7	7	7	**21**
5	Fyzické napadení (beze zbraně)	7	7	7	**21**
6	Výhružka chladnou zbraní	6	5	7	**18**
7	Napadení chladnou zbraní s cílem ohrozit jednu vybranou osobu	6	3	6	**15**
8	Napadení chladnou zbraní s cílem ohrozit velký počet osob	6	2	6	**14**
9	Požár – technická závada/nedbalost	7	7	7	**21**
10	Žhářský útok s cílem ohrozit jednu vybranou osobu	4	5	6	**15**
11	Žhářský útok s cílem usmrtit velký počet osob	4	4	5	**13**
12	Použití zápalné láhve	3	2	6	**11**
13	Aktivní střelec	4	3	7	**14**
14	Útok střelnou zbraní s cílem ohrozit jednu vybranou osobu	4	2	6	**12**
15	Útok střelnou zbraní s cílem ohrozit velký počet osob	4	3	5	**12**
16	Nájezd atentátníka automobilem do objektu	5	2	7	**14**
17	Výhružka útoku s NVS	1	2	4	**7**
18	Sebevražedný útok s použitím NVS	1	2	6	**9**
19	Použití NVS s cílem usmrtit velký počet osob	1	2	5	**8**
20	NVS v zaparkovaném voze	1	2	6	**9**
21	Umístění NVS u zásobníku kyslíku	1	2	4	**7**
22	Umístění NVS u zdroje tepla nebo el. energie	1	2	4	**7**
23	Použití nebezpečné biologické látky	2	1	5	**8**

Z výše uvedené Tab. 3 vyplývá, že nejvyšší míra pravděpodobnosti výskytu byla v této analýze přiřazena verbálnímu a fyzickému napadení beze zbraně. To je způsobeno především tím, že potenciální pachatel ke svému činu nepotřebuje žádné zbraně a je možné zaútočit téměř kdekoli. Z praxe je známo, že tyto uvedené druhy rizika jsou ve zdravotnickém prostředí velmi časté. Dalším významným rizikem, kterému byla přiřazena vysoká míra pravděpodobnosti, byla výhružka NVS a využívání tzv. chladných zbraní (bodné, sečné nebo tupé).

Dalším krokem při zpracování analýzy je stanovení závažnosti negativních dopadů jednotlivých rizik na dotčený objekt. V této části jsou stanoveny dopady rizik na životech (Ž), objektech (O), finanční dopad (F) a dopad na přímo zasažené společenství (ZS). Dopady jsou stejně jako míra pravděpodobnosti hodnoceny kvalifikovaným odhadem na škále od 1 do 7. Bodovací škály jsou uvedeny v tabulkách v Příloze č. 5. Výsledné hodnoty jednotlivých parametrů dopadů a jejich celkové hodnoty jsou uvedeny níže v Tab. 4.

Celkové dopady jednotlivých jsou vypočteny na základě vzorce č. 2.

$$N = Ž + O + F + ZS \qquad (2)$$

kde:

Ž – dopady na životech a zdraví;

O – dopady na objektu;

F – finanční dopady;

ZS – přímo zasažené společenství.

Z Tab. 4 je možné odvodit, že nejzávažnější dopady představují především požáry z nedbalosti, jednotlivé typy žhářských útoků a rizika týkající se využívání NVS odlišným způsobem. Na druhou stranu žádné nebo minimální dopady přestavují krádeže, vloupání, vandalismus nebo verbální či fyzické napadení.

Tab. 4 – Analýza dopadů [autor]

Č.	Riziko	Specifikace útoků		Analýza dopadů				Celkový dopad (N)
		Lokalizace	Načasování	Ž	O	F	ZS	
1	Vandalismus	Uvnitř /Těsná blízkost	Celý den	1	2	3	1	**7**
2	Krádež	Uvnitř	Celý den	1	1	3	1	**6**
3	Vloupání	Uvnitř	Mimopracovní	1	1	3	2	**7**
4	Verbální napadení	Uvnitř	Pracovní doba	1	1	1	1	**4**
5	Fyzické napadení (beze zbraně)	Uvnitř	Pracovní doba	2	1	2	1	**6**
6	Výhružka chladnou zbraní	Uvnitř	Pracovní doba	1	1	2	1	**5**
7	Napadení chladnou zbraní s cílem ohrozit jednu vybranou osobu	Uvnitř	Pracovní doba	2	1	2	3	**8**
8	Napadení chladnou zbraní s cílem ohrozit velký počet osob	Uvnitř	Pracovní doba	3	1	2	3	**9**
9	Požár – technická závada/nedbalost	Uvnitř	Pracovní/mimopracovní	6	6	7	6	**25**
10	Žhářský útok s cílem ohrozit jednu vybranou osobu	Uvnitř	Pracovní doba	6	6	6	4	**22**
11	Žhářský útok s cílem usmrtit velký počet osob	Uvnitř	Pracovní doba	7	6	6	4	**23**
12	Použití zápalné láhve	Uvnitř	Pracovní doba	6	6	6	6	**24**
13	Aktivní střelec	Uvnitř	Pracovní doba	6	5	6	6	**23**
14	Útok střelnou zbraní s cílem ohrozit jednu vybranou osobu	Uvnitř	Pracovní doba	6	5	5	6	**22**
15	Útok střelnou zbraní s cílem ohrozit velký počet osob	Uvnitř	Pracovní doba	7	5	6	6	**24**
16	Nájezd atentátníka automobilem do objektu	Těsná blízkost	Pracovní doba	5	4	5	5	**19**
17	Výhružka útoku s NVS	Uvnitř	Pracovní doba	6	3	5	6	**20**
18	Sebevražedný útok s použitím NVS	Uvnitř	Pracovní doba	7	7	6	6	**26**
19	Použití NVS s cílem usmrtit velký počet osob	Uvnitř	Pracovní doba	7	7	6	6	**26**
20	NVS v zaparkovaném voze	Vnější prostor	Pracovní doba	6	5	6	6	**23**
21	Umístění NVS u zásobníku kyslíku	Uvnitř	Pracovní doba	7	6	5	6	**24**
22	Umístění NVS u zdroje tepla nebo el. energie	Uvnitř	Pracovní doba	7	4	5	6	**22**
23	Použití nebezpečné biologické látky	Uvnitř	Pracovní doba	5	5	5	4	**19**

Poslední fází provedené analýzy rizik je stanovení výsledné úrovně ohrožení jednotlivých rizik. Celková míra ohrožení R byla vypočítána ze vzorce č. 3.

$$R = P * N \qquad (3)$$

kde:

P – celková pravděpodobnost vzniku;

N – celkové dopady rizik.

V Tab. 6 je poté spočtena celková míra ohrožení u jednotlivých rizik. Nejnižší míra ohrožení byla stanovena u verbálního napadení a zastrašení chladnou zbraní. Na druhou stranu nejvyšší míra ohrožení byla zjištěna u jednotlivých metod žhářských útoků.

5.5 Hodnocení rizik

Závěrečnou činností posuzování rizik je tzv. hodnocení rizik. Na základě výsledných hodnot celkové míry ohrožení došlo k samotnému přiřazení přijatelnosti daného rizika. Hodnocení rizik vycházelo z tabulky přijatelnosti viz Tab. 5.

Tab. 5 – Tabulka přijatelnosti [13]

R	Míra rizika	Přijatelnost
12 – 90	Bezvýznamné	Přijatelné
91 – 180	Akceptovatelné	
181 – 288	Mírné	Podmínečně přijatelné
289 – 388	Významné	Nepřijatelné
389 – 588	Nežádoucí	

Na základě Tab. 5 byla provedena komparace jednotlivých hodnot s výsledky, které jsou uvedeny v Tab. 6. Status nepřijatelného rizika byl přiřazen požáru, žhářským útokům a aktivnímu střelci, kde se celková míra rizika R pohybovala okolo hodnoty 300 až 500. Do kategorie podmínečně přijatelné lze zařadit násilné útoky střelnou zbraní, využívání NVS, najetí atentátníka automobilem do objektu nebo výhružku útokem s použitím NVS. Jako přijatelné riziko vyšlo verbální a fyzické napadení beze zbraně, využití chladné zbraně nebo umístění NVS v provozních prostorech nemocnice.

Na základě průzkumu a výsledků zpracovaného posouzení rizik budou v této diplomové práci vytvořeny bezpečnostní scénáře pouze pro nepřijatelná rizika, tedy pro požáry a útok aktivního střelce. Z důvodu velké pravděpodobnosti výskytu (viz Tab. 3) bude navíc vytvořen bezpečnostní scénář na verbální a fyzické napadení, které může předcházet ozbrojenému útoku.

Tab. 6 – Celková úroveň rizika včetně hodnocení [autor]

Č.	Riziko	Výsledky		Celková míra ohrožení (R)	Hodnocení
		Pravděpodobnost (P)	Dopady (N)		
1	Vandalismus	21	7	**147**	Přijatelné
2	Krádež	21	6	**126**	Přijatelné
3	Vloupání	20	7	**140**	Přijatelné
4	Verbální napadení	21	4	**84**	Přijatelné
5	Fyzické napadení (beze zbraně)	21	6	**126**	Přijatelné
6	Výhružka chladnou zbraní	18	5	**90**	Přijatelné
7	Napadení chladnou zbraní s cílem ohrozit jednu vybranou osobu	15	8	**120**	Přijatelné
8	Napadení chladnou zbraní s cílem ohrozit velký počet osob	14	9	**126**	Přijatelné
9	Požár – technická závada/nedbalost	21	25	**525**	Nepřijatelné
10	Žhářský útok s cílem ohrozit jednu vybranou osobu	15	22	**330**	Nepřijatelné
11	Žhářský útok s cílem usmrtit velký počet osob	13	23	**299**	Nepřijatelné
12	Použití zápalné láhve	11	24	**264**	Podmínečně přijatelné
13	Aktivní střelec	14	23	**322**	Nepřijatelné
14	Útok střelnou zbraní s cílem ohrozit jednu vybranou osobu	12	22	**264**	Podmínečně přijatelné
15	Útok střelnou zbraní s cílem ohrozit velký počet osob	12	24	**288**	Podmínečně přijatelné
16	Nájezd atentátníka automobilem do objektu	14	19	**266**	Podmínečně přijatelné
17	Výhružka útoku s NVS	7	20	**140**	Přijatelné
18	Sebevražedný útok s použitím NVS	9	25	**225**	Podmínečně přijatelné
19	Použití NVS s cílem usmrtit velký počet osob	8	26	**208**	Podmínečně přijatelné
20	NVS v zaparkovaném voze	9	23	**207**	Podmínečně přijatelné
21	Umístění NVS u zásobníku kyslíku	7	24	**168**	Přijatelné
22	Umístění NVS u zdroje tepla nebo el. energie	7	22	**154**	Přijatelné
23	Použití nebezpečné biologické látky	8	19	**152**	Přijatelné

6 Základní návrh opatření FO

Jedním z významných nedostatků, kterým čelí zdravotnické organizace v souvislosti s používáním dnešní bezpečnostní technologie, je nedostatečné pochopení možností pořízeného systému ze strany koncového uživatele. Často chybí zpracovaná koncepce bezpečnosti definující provozní principy, které pomohou určit využívání vhodných funkcí STO, zajistí jejich optimální využití a také určuje způsob řešení školení bezpečnostních pracovníků k vykonání efektivního zásahu při vzniku mimořádné události. Za jejím vytvořením by měly stát klíčové složky organizace včetně zástupců bezpečnostního oddělení, informačních technologií (IT), lidských zdrojů a řízení rizik. [47]

Následující podkapitoly popisují základní požadavky na implementaci bezpečnostní opatření v areálech nemocnic včetně režimových opatření. Jedná se pouze o výčet základních opatření, která by měla být v nemocnicích implementována. Konkrétní opatření jsou závislá na skutečném dispozičním a provozním řešení objektu.

Řízení fyzické ochrany

Prvním krokem k zajištění vhodného využití všech odvětví fyzické ochrany je implementace tzv. „*Řízení fyzické ochrany*“. Jedná se o aktivity, které souvisejí s plánováním, rozhodováním, řízením a koordinací bezpečnostních opatření. Řízení by mělo být uplatňováno ve čtyřech rovinách, a to v rámci přípravy na MU, při vzniku MU, v období odstraňování škod a při implementaci nových opatření. Každá nemocnice musí mít zpracovanou bezpečnostní dokumentaci a na ní navazující vnitřní předpisy. Jedná se o bezpečnostní politiku a bezpečnostní standard, který bude definovat minimální požadavky na rozsah opatření v rámci FO. Dále musí být v areálech nemocnic definována pracoviště se zvláštním režimem. V rámci kontroly vhodného nastavení všech opatření je doporučeno provádět bezpečnostní audity a penetrační testy.

V rámci řízení FO je potřeba zřídit bezpečnostní management, za jehož činnost bude zodpovídat bezpečnostní manažer. Tento interní orgán bude mít na starost udržování bezpečnostní politiky, odpovědnost za úroveň a kvalitu implementovaných opatření, realizaci vhodných opatření na základě druhu vzniklé MU apod.

Ve všech budovách je pro ochranu přítomných osob vhodné vytipovat místnosti, které budou sloužit k improvizovanému ukrytí (dle metodiky MVCR se tyto prostory také

nazývají SAFE HAVEN). Místnosti improvizovaného ukrytí by měly v co největší míře splňovat základní kritéria. Prostory by měly být vybudované z pevných a nejlépe z požárně odolných materiálů, vstupy musí být vybaveny plnými, uzamykatelnými dveřmi, které budou mít požadovanou mechanickou odolnost. Samotný prostor by neměl být vybaven skleněnými plochami. Prostory mohou být také vybaveny prostředky osobní ochrany např. pepřovými spreji. Tato místa budou v případě vzniku MU využívána jako bezpečnostní kryt před případným pachatelem nebo NVS v objektu.

Mechanické zábranné prostředky

Areál nemocnice by měl být po celém svém perimetru zajištěn dostatečně vysokým oplocením (minimálně 1,8 m) s vrcholovou zábranou se třemi sledy žiletkového drátu a podhrabovou překážkou. Vegetace kolem perimetru by měla být upravena tak, aby nebránila monitoringu perimetru.

Na všech vstupech do objektů v areálu, především na vnějších neveřejných vstupech, by měl být instalován sjednocený bezpečnostní uzamykací systém (zámek, kování, vložka) v provedení knoflík-klika. Vhodným řešením je využití mechanických, elektromechanických a elektromotorických samozamykacích zámků s panikovou funkcí, které jsou vždy v případě uzavření dveří automaticky uzamčeny. Primárně je na všech vnějších vstupech do objektů s ohledem na činnost ostrahy při řešení MU doporučeno realizovat systém generálního a hlavního klíče. Systém generálního klíče je vhodné realizovat s využitím mechatronických klíčů (klíče s elektronickým čipem). Ve vnitřních prostorách je vhodné pro zajištění úniku a evakuace všechny vstupy na jednotlivá oddělení opatřit elektromechanickými zámky s inverzní funkcí, kdy tyto zámky jsou v klidovém režimu (bez napětí) stále otevřeny. Konkrétní využití těchto zámků je popsáno v jednotlivých bezpečnostních scénářích v kapitole č. 7. Vstupní dveře na jednotlivá oddělení by měly minimálně splňovat bezpečnostní třídu RC 2 dle ČSN EN 1627. Pro možnost případného ukrytí je v nemocnicích doporučeno minimalizovat skleněné plochy, popřípadě je doporučeno využívat mléčné, odolné sklo opatřené bezpečnostní fólií. Skleněné plochy na sesternách, sloužící k pozorování pacientů nebo ke komunikaci s návštěvníky, by měly být opatřeny minimálně bezpečnostní fólií.

Na hlavních vstupech do jednotlivých objektů by mělo být pro minimalizování rizika zajištěno automatické přepínání vstupních režimů. V provozní době bude volný vstup

povolen automaticky, zatímco po automatickém přepnutí do mimoprovozní doby bude vstup zajištěn za pomoci systému ESKV. Na hlavních vstupech pro veřejnost, kde by mohla být vyšší kumulace osob, by měly být instalovány systémy pro zamezení vjezdu automobilem, například dálkově ovladatelné dopravní sloupy s dostatečnou odolností proti nárazu a dostatečnou výsuvnou výškou.

V objektech nemocnic je vhodné instalovat odpadkové koše, které jsou odolné proti explozím, nebo které mají malý vhazovací otvor, a to z důvodu zabránění vhození nebezpečných předmětů.

Poplachové zabezpečovací a tísňové systémy

V objektech areálu nemocnice by měl být instalován systém jednotného stupně zabezpečení dle ČSN EN 50131 ed.2 (minimálně v rozsahu pro stupeň zabezpečení 3).

Všechny vstupy/vjezdy na perimetru areálu je vhodné střežit systémem PZTS. Jednotlivé vstupy je doporučeno rozdělit na vstupy pro veřejnost a na vstupy pro zaměstnance/dodavatele. Vstupy pro veřejnost musí být v provozní době odstřeženy. V neprovozní době musí dojít u těchto vstupů k automatickému zastřežení. Tyto vstupy/vjezdy bude možné odstřežit na místě pouze za pomoci systému ESKV (čtečky) nebo vzdáleně z dohledového centra. U vstupů pro zaměstnance/dodavatele je vhodné zajisti, aby byly trvale zastřeženy. Jejich odstřežení a otevření bude poté zajištěno prostřednictvím systému ESKV.

Na všech venkovních vstupech by měla být instalována plná plášťová ochrana (instalace magnetických kontaktů a detektorů tříštění skla). Dále by měly být instalovány MK na všech otevíratelných oknech v technologických místnostech a místnostech důležitých pro chod nemocnice, které jsou situovány níže než 2,5 m nad terénem nebo jsou přístupné z různých přístupových tras (hromosvod, okap, žebřík). Prostory, které jsou důležité z hlediska chodu nemocnice nebo které jsou níže, než je stanovena výška nad okolním terénem, a jsou situovány do vnějšího prostoru, je vhodné vybavit prostorovými detektory.

V rámci systému PZTS je vhodné objekty vybavit pevnými tísňovými hlásiči, které by měly být instalovány především v čekárnách, na sesternách jednotlivých oddělení, v ordinacích lékařů, na sekretariátu ředitele a v kanceláři ředitele. Přenosnými tísňovými

hlásiči by měli být vybaveny především vrchní sestry jednotlivých oddělení, lékaři a pracovníci ostrahy.

Elektronické systémy kontroly vstupu

Pro zajištění kontroly vstupu v areálech nemocnic je doporučeno využívat systémy kombinující funkce PZTS a ESKV. Oproti odděleným systémům nabízí uživateli několik benefitů. Jako příklad lze uvést nativní ovládání PZTS prostřednictvím identifikačních prvků ESKV jednotlivými uživateli. Ti jsou oprávněni zastřežovat/odstřežovat jednotlivé podsystémy PZTS na základě jejich přiřazených práv. Dále je možné kombinací systémů zajistit blokování otevření dveří do zastřežené oblasti za pomoci el. zámků. Tímto je možné snížit počty planých poplachů. Zmíněné benefity výrazně usnadňují současné ovládání těchto dvou systémů, kdy jednotliví uživatelé nejsou vázáni na součinnost s dispečerem na dohledovém centru.

Systém by měl být instalován na všech vnějších vstupech a vjezdech do areálu. Dále by měly být kontrolovány všechny vstupy do jednotlivých budov jak veřejně přístupných (mimo provozní dobu), tak veřejně nepřístupných. Řízení přístupu by mělo být zajištěno také na vstupech do uzavřených pracovišť, jako jsou laboratoře, operační sály, technologické místnosti, sklady apod. Na výše zmíněných vstupech je vhodné kontrolovat jejich uzavření. Pokud budou dveře otevřené po dobu delší, než je stanoveno (například 1 minuta), dojde k vyhlášení poplachu na dohledové centrum nemocnice.

Dohled nad systémem musí být umožněn z dohledového centra areálu nemocnice. Dispečer dohledového centra musí dostávat informace minimálně v níže uvedeném rozsahu:

- překročení maximální povolené doby otevření jednotlivých prostorů;
- opakované zamítnutí vstupu;
- využití vyřazeného identifikačního prvku;
- otevření bez užití přístupového prvku (násilné otevření);
- sabotáž přístupové čtečky nebo jiných částí ESKV;
- detekce poruchy systému.

Systém musí být schopen ovládat elektromechanické nebo elektromotorické zámky za účelem blokace nebo otevření zámků pro omezení pohybu potenciálního pachatele, nebo pro otevření dveří pro možný únik nebo ukrytí osob.

Evakuační rozhlas

Evakuační rozhlas by měl být instalován ve všech objektech areálu nemocnice. Rozhlas by měl být rozdělen do jednotlivých zón, kdy do každé zóny je umožněno předat odlišnou digitální zprávu. Systém musí umožňovat spouštění přednastavených digitálních zpráv, které by měly být nastaveny minimálně v takovém rozsahu, jak je uvedeno v Tab. 7. Tyto digitální zprávy jednoznačně informují proškolený personál nemocnice o vzniklé situaci, který na základě těchto zpráv provede vhodná režimová opatření. Předávání poplachových informací personálu v kódech omezí vzniku paniky mezi návštěvníky nemocnice. Dále by měl systém umožňovat hovořit do jednotlivých zón za pomoci mikrofonu z dohledového centra nemocnice. Příklad celé digitální zprávy může mít podobu např.: „*Prosím pozor! V objektu XXX je vyhlášen Kód 1. Prosíme zaměstnance nemocnice o provedení příslušných opatření.*“

Tab. 7 – Návrh digitálních zpráv pro evakuační rozhlas [autor, upraveno z [13]]

Digitální zpráva	Význam	Definice
„ …Kód 1… “	Záměrný útok	V objektu došlo k úmyslnému útoku s cílem ohrozit zdraví nebo život přítomných osob. Je nutné zajistit okamžitou invakuaci všech osob v objektu. Můžeme zde zahrnout např. aktivního střelce.
„ …Kód 2… “	Hrozí ohrožení života	Jedná se o situaci, kdy MU pouze hrozí, ale ještě nenastala a není jisté, zda nastane. Můžeme zde zahrnout např. výhružku NVS.
„ …Kód 3… “	Technická závada s možností ohrožení života	Došlo k MU, která nemusí být úmyslná, ale může ohrožovat životy a zdraví přítomných osob. Je nutné zahájit okamžitou evakuaci. Můžeme zde zahrnout požár.
„ …Kód 4… “	Odvolání nebezpečí	Informování personálu nemocnice, že dříve vyhlášená digitální zpráva již nehrozí.
„Uzamkněte, prosím, své pokoje a nevycházejte“	Záměrný útok	V objektu došlo k úmyslnému útoku. Zpráva bude vysílána na lůžkových pokojích. Pouze pro případ aktivního střelce.
„V objektu byla spuštěna bezpečnostní mlha“	Spuštění zamlžovacího zařízení	V objektu došlo k úmyslnému útoku. Pro snížení následků byla v objektu spuštěna bezpečnostní mlha.

Elektronická požární signalizace

Parametry, které určují rozsah a způsob instalace systému EPS, jsou jasně definovány v aktuálně platných normativních a právních předpisech. Tyto parametry musí být řádně dodrženy. Nad rámec běžných požadavků je doporučeno tento systém připojit do integračního nadstavbového softwaru pro zajištění vyššího přehledu nad vzniklou MU a k umožnění rychlejšího předání informace o poplachu na pracovníky dohledového centra.

Dohledové videosystémy

V celém areálu nemocnice je doporučeno instalovat jednotný dohledový videosystém. Ten je možné realizovat lokálními záznamovými servery, systémem centrálního dohledu a videomanagementem. Celý systém musí být instalován v souladu s normami řady ČSN EN 62676, požadavky nařízení Evropského parlamentu a Rady (EU) 2016/679 a požadavky zákona č. 110/2019 Sb., o zpracování osobních údajů. Pro zajištění dostatečného přehledu nad okolnostmi v areálu nemocnice je vhodné systém VSS instalovat zejména v níže zmíněných prostorách:

- pracoviště dohledového centra nemocnice, technologické prostory související s provozem nemocnice;
- všechny vstupy do objektů, hlavní chodby, čekárny, sesterny;
- prostory, kde jsou uchovány cennosti pacientů;
- sklady léčiv, narkotik, lékárny a další sklady s cenným zbožím;
- přijímací střediska, zásobovací prostory;
- dětská oddělení (pediatrie), psychiatrické oddělení a jemu podobné;
- perimetr, parkoviště a garáže.

Doba zálohy pořízeného záznamu by měla být nastavena minimálně na 10 dní.

Dohledové centrum nemocnice

Všechny instalované bezpečnostní systémy je doporučeno vyvést na dohledové centrum nemocnice, kde budou dispečery přijímány a řešeny jejich poplachové a poruchové stavy. Dohledové centrum bude zároveň fungovat jako ohlašovna požáru. Systémy budou integrovány do jednotného integračního nadstavbového softwaru, který bude umožňovat komplexní přehled nad současnou situací v areálu nemocnice. Dále bude mít dohledové centrum vyvedenou samostatnou klapku skrze vnitřní komunikační systém,

která bude sloužit jako jedna z možností, jak informovat dispečera o vzniklé mimořádné události. Na dohledovém centru musí by měly být přítomny minimálně dvě osoby. Dohledové centrum by mělo v co největší míře respektovat podmínky, které jsou stanoveny normou ČSN EN 50518.

Níže uvedená Tab. 8 uvádí rozdělení vybraných poplachových stavů dle priority a navrhuje logické vazby na STO a EPS v objektech nemocnic. Návrh propojení jednotlivých bezpečnostních systémů je součástí Přílohy č. 7.

Tab. 8 – Prioritní stavy STO a EPS [autor, upraveno z [13]]

Systém	Priorita	Signalizovaný stav	Návazná akce
PZTS	Vyšší	○ Detekce narušení plášťové, prostorové a předmětové ochrany ○ Detekce sepnutí tísňového hlásiče ○ Detekce sabotáže	○ Přenos stavu na dohledové centrum ○ Sepnutí systému VSS v nejbližších místech ○ V případě nutnosti vyhlásit digitální zprávu evakuačním systémem, popř. systémem sestra-pacient ○ Využití systému ESKV pro otevření/uzavření prostorů ○ Možnost "trasování" pachatele prostřednictvím MK a VSS
	Nižší	○ Detekce poruchy systému ○ Detekce opomenutí zastřežení	○ Přenos stavu na dohledové centrum ○ Sepnutí systému VSS v nejbližších místech
VSS	Vyšší	○ Vyhlášení poplachu na základě videoanalytických funkcí ○ Detekce zakrytí kamery	○ Přenos stavu na dohledové centrum ○ Sepnutí systému VSS v nejbližších místech ○ V případě nutnosti vyhlásit digitální zprávu evakuačním systémem ○ Využití systému ESKV pro otevření/uzavření prostorů ○ Možnost "trasování" pachatele
	Nižší	○ Detekce poruchy systému ○ Detekce otočení kamery	○ Přenos stavu na dohledové centrum ○ Sepnutí systému VSS v nejbližších místech
ESKV	Vyšší	○ Detekce překročení maximální povolené doby otevření dveří ○ Detekce otevření střežených prostorů při neoprávněné autorizaci ○ Detekce zakázané karty ○ Detekce sabotáže	○ Přenos stavu na dohledové centrum ○ Sepnutí systému VSS v nejbližších místech ○ V případě nutnosti vyhlásit digitální zprávu evakuačním systémem ○ Využití systému ESKV pro otevření/uzavření prostorů ○ Možnost "trasování" pachatele prostřednictvím MK a VSS
	Nižší	○ Detekce poruchy systému ○ Detekce opakované chybné autorizace	○ Přenos stavu na dohledové centrum ○ Sepnutí systému VSS v nejbližších místech
EPS	Vyšší	○ Hlášení požáru	○ Přenos stavu na dohledové centrum ○ Sepnutí systému VSS v nejbližších místech ○ Vyhlásit digitální zprávu evakuačním systémem a systémem sestra-pacient
	Nižší	○ Detekce poruchy systému	○ Přenos stavu na dohledové centrum ○ Sepnutí systému VSS v nejbližších místech

7 Bezpečnostní scénáře pro nemocnice

Scénář je možné obecně charakterizovat jako systémový model, který je aplikován v řízení. Jeho úkolem je popsat budoucí rozvoj nějaké situace v rozdílných podobách, kdy vývoj situace je závislý na okolních podmínkách. Zaměřuje se na postup ve variantní podobě, který napodobuje procesy a mechanismy v systému. Hlavním cílem scénářů je popis MU a jejích kritických bodů, ve kterých je nezbytné učinit rozhodnutí a provést postupy, které budou vývoj situace ovlivňovat. Důsledky rozhodnutí jsou uvedeny jako volitelné výběry mezi konečnými stavy budoucnosti. [30]

Scénář tvoří soubor předem připravených a propojených opatření a činností, které jsou mezi sebou navzájem logicky provázány, pro zajištění vysoké efektivity a ekonomičnosti navržených opatření. [30]

Cílem diplomové práce je navrhnout bezpečnostní scénáře na předem vybrané mimořádné události v nemocničních zařízeních. Jednotlivé scénáře se ve své první části zabývají způsobem detekce mimořádné události a přenosem poplachové zprávy na dohledové centrum nemocnice. Dále popisují postup aktivace či deaktivace jednotlivých systémů technické ochrany, a to jak v zóně útoku, tak mimo ni. V návaznosti na aplikaci těchto postupů scénáře určují aplikování jednotlivých režimových opatření pro zajištění účinného zásahu FOs nebo IZS v případě vzniku mimořádné události. Scénáře jsou vytvořeny v podobě vývojových diagramů, a to na tyto vybrané mimořádné události:

- verbální a fyzické napadení (beze zbraně);
- ozbrojený útok:
  - ambulantní oddělení;
  - lůžkové oddělení.
- požár.

Jelikož v rámci diplomové práce nebyl posuzován žádný konkrétní objekt, jsou bezpečnostní scénáře navrženy pouze v obecné rovině. V praxi je potřeba scénáře a jednotlivé požadavky modifikovat dle skutečných možností a provozních požadavků jednotlivých objektů a oddělení nemocnic.

7.1 Verbální a fyzické napadení

Tato kapitola je zaměřena na vytvoření scénáře popisující možnou variantu aplikování, zejména režimových opatření spolu s funkcemi instalovaných STO a FOs při verbálním nebo fyzickém útoku. Scénář popisuje situaci, kdy pachatel útočí na přítomné osoby buď verbálně, nebo fyzicky, ale bez využití útočného předmětu. Samotné řešení útoku se bude pokaždé odvíjet od aktuální situace.

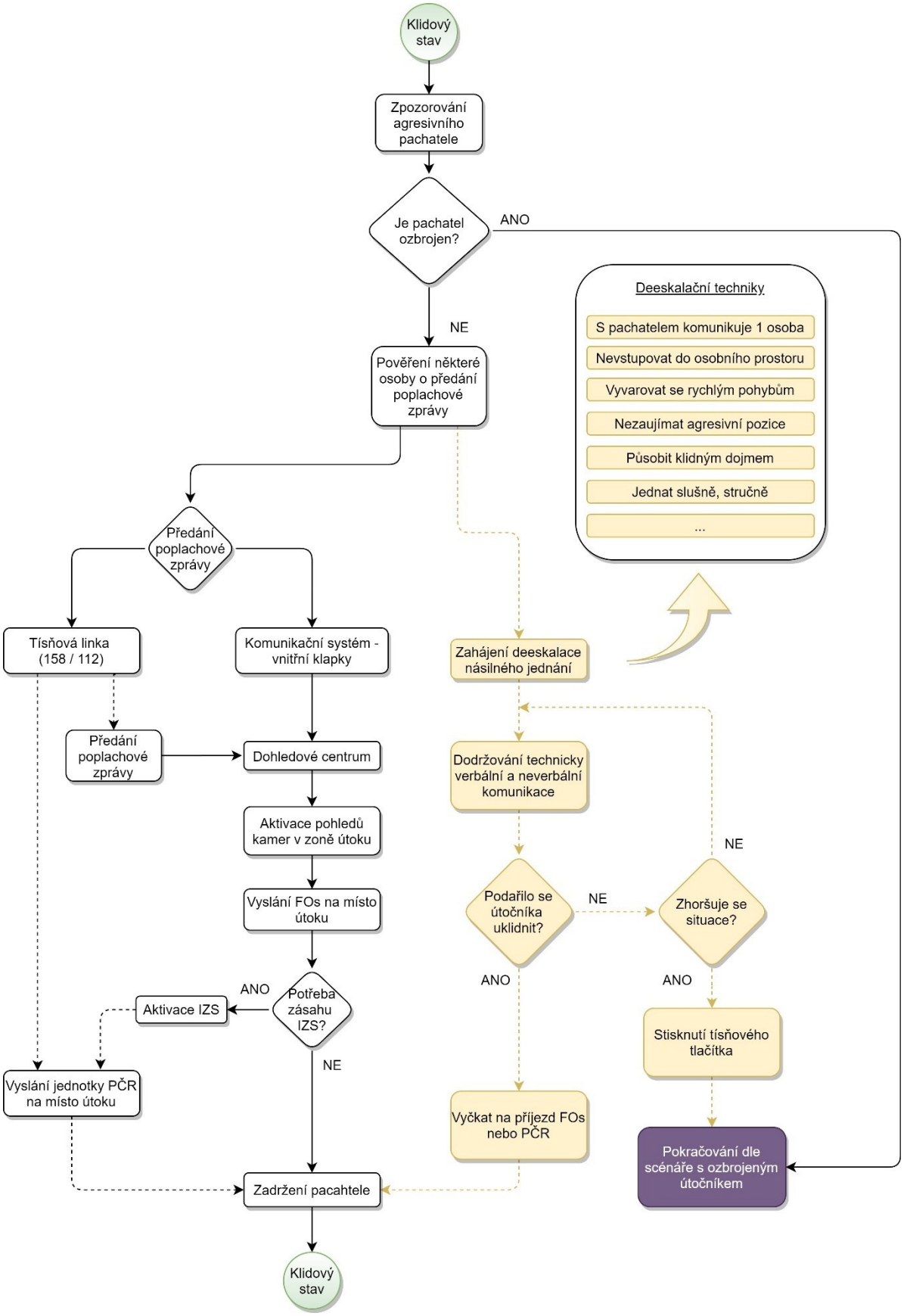
Jestliže nastane situace, že některá z přítomných osob v nemocnici bude verbálně nebo fyzicky napadena neozbrojeným pachatelem, bude v ideálním případě poplachová informace předána přímo na dohledové centrum nemocnice prostřednictvím vnitřních komunikačních systémů (vnitřní klapky). Přivolání pomoci by mělo proběhnout nejlépe druhou osobou a v tichosti. Druhou variantou je využití tísňových linek 158 nebo 112. Jestliže bude využito tísňové linky, je potřeba zajistit, aby daná složka IZS ihned informovala dohledové centrum nemocnice. Po přijetí poplachové zprávy si dispečer dohledového centra zobrazí pohledy z kamer v daném prostoru a na místo útoku vyšle FOs nemocnice. Pokud to situace bude dovolovat, tak je pro předání poplachové informace doporučeno nevyužívat tísňové tlačítko, jelikož při jeho aktivaci je následně uzamčena zóna útoku. Tyto úkony by mohly agresivního pachatele rozrušit a mohlo by dojít ke zhoršení situace.

Pro zvládnutí situace a zklidnění útočníka je potřeba, aby byl personál nemocnice seznámen s využíváním deeskalačních technik. Jednající osoba, která je v konfrontaci s pachatelem, by měla strhnout veškerou pozornost útočníka na sebe. S pachatelem je nutné komunikovat tak, aby nedocházelo ke zvyšování pachatelovy agresivity. Jednatel musí komunikovat slušně a nesmí se nechat vyprovokovat ke slovní nebo fyzické konfrontaci. Cílem vzájemné komunikace s pachatelem je jeho zklidnění na takovou míru, aby bylo možné s pachatelem především jednat, eventuálně jej zadržet. Přímý útok proti pachateli může být veden pouze s jistotou, že pachatel není ozbrojen a je zde vysoká pravděpodobnost jeho zadržení. Níže uvedené body popisují verbální a neverbální deeskalační technicky, jejichž aplikaci lze doporučit k jednání s útočníkem [13]:

- s pachatelem mluví pouze jedna osoba;
- nevstupovat do osobního prostoru pachatele;
- vyvarovat se rychlým pohybům;
- nezaujímat agresivní pozice (ruce v bok, ruce v pěst, nevhodné náznaky);

- pokud to situace dovoluje, požádat agresora, aby si sedl;
- snažit se působit klidným dojmem;
- jednat slušně, bez vulgárních výrazů, stručně;
- vyhýbat se rozkazům;
- nevyžadovat po pachateli okamžitou odpověď;
- vyslechnout agresora a vystupovat chápavým dojmem;
- využívat laskavého a empatického chovaní;
- snažit se klást vhodné otázky, které poskytují čas pro zásah FOs nebo PČR.

V případě, že by agresivní osoba vytáhla útočnou zbraň nebo by pro svůj útok využila jiný útočný předmět, bude situace řešena dle kapitoly 7.2. Na Obr. 2 je vytvořen obecný scénář popisující možné řešení verbálního nebo fyzického útoku neozbrojeným pachatelem. Čárkovaně označené postupy budou probíhat paralelně s dalšími opatřeními. S ohledem na čitelnost je vytvořený scénář zobrazen na samostatné straně.



Obr. 2 – Vývojový diagram postupu při verbálním a fyzickém napadení [autor]

7.2 Ozbrojený útok

V této podkapitole byl vytvořen scénář popisující posloupnost uplatňování vybraných funkcí jednotlivých STO a dalších režimových opatření vedoucí k zajištění ozbrojeného pachatele s minimálními dopady na životech a zdraví přítomných osob. Útok je v rámci této kapitoly chápan jako protiprávní čin, který je páchán osobou (pachatelem) proti chráněnému zájmu. Ozbrojený útočník využívá zbraň pro ohrožení života a zdraví jiných osob. Zmíněné osoby nedisponují žádnými morálními zábranami a jejich útok může být směřován na jednu předem vytipovanou oběť, nebo může být jejich záměrem zranit či usmrtit co největší počet osob. Přítomné osoby by měly brát v úvahu, že chování útočníka je ve velké míře závislé na vývoji situace. Proto bude především záležet na reakci přítomných osob v prostoru a na dalších rušivých podnětech, jako je např. křik osob, obrané protiútoky, sirény, evakuační zprávy apod. Z důvodu omezeného rozsahu diplomové práce je níže vytvořený scénář zaměřen pouze na situace, kdy útočník zahájí útok v prostorách ambulantní péče nebo na lůžkovém oddělení, kde lze s ohledem na vysokou kumulaci osob a omezenou mobilitu pacientů předpokládat největší pravděpodobnost provedení útoku.

Ozbrojený pachatel může být v objektu zpozorován třemi způsoby, a to osobami v místnosti (pacienti, personál, návštěva apod.), dispečerem na dohledovém centru prostřednictvím instalovaných kamer nebo může být systémem VSS detekován automaticky pomoci pokročilé videoanalytické funkce „detekce zbraně“. Poplachová informace o útočníkovi musí být neprodleně předána dispečerovi na dohledové centrum nemocnice. K tomu může dojít několika způsoby:

- tísňové hlásiče PZTS (přenosné, osobní s lokalizátorem);
- systém VSS (videoanalytická funkce);
- komunikační prostředky nemocnice (vnitřní klapky);
- informování tísňové linky (tel. číslo: 112, 158), která informaci předá na dohledové centrum nemocnice.

Jestliže se pachatel s útočnou zbraní dostane až do některého z objektů nemocničního areálu, prví možností je využití kombinace lidského činitele a tísňových hlásičů (dále jen TH), které budou instalovány jako součást systému PZTS. TH by měly být umístěny zejména na všech sesternách, vrátnicích a čekárnách. Vhodným řešením je také využívání osobních TH s lokalizátorem, kterými by měli být vybaveni především zdravotní sestry,

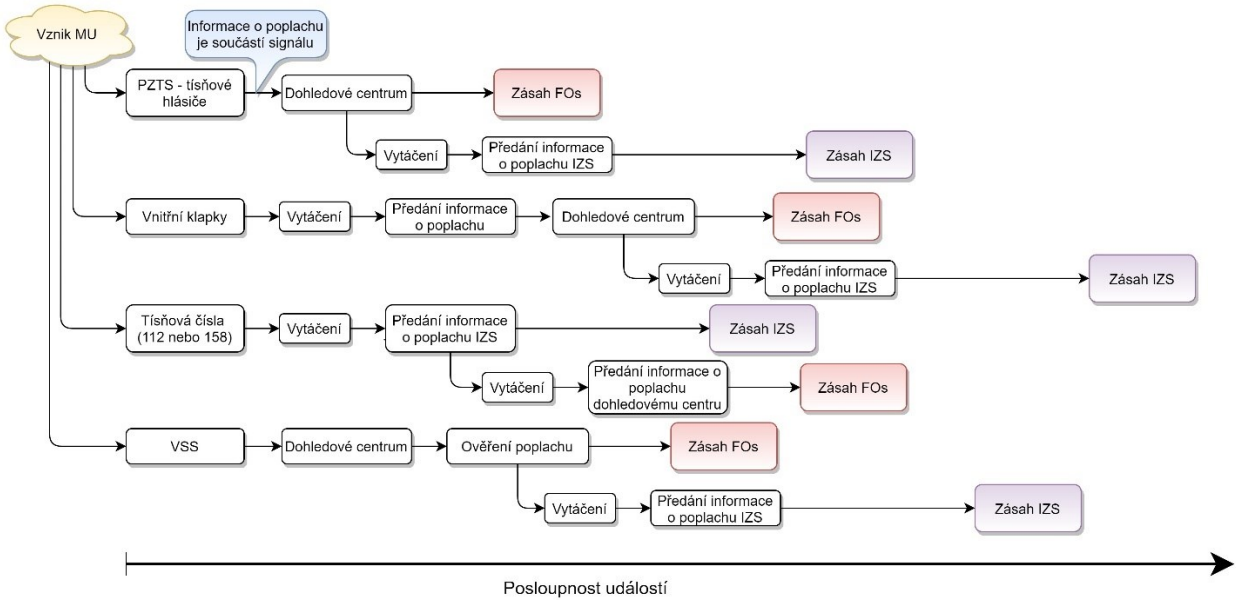
lékaři a pracovníci FOs. Pevné TH musí být jasně rozlišitelné od tlačítkových hlásičů systému EPS a je vhodné je označit informační tabulkou. TH musí být v čekárně instalován takového typu, aby nedošlo k jeho nechtěné aktivaci (možný typ TH je zobrazen na Obr. 3). Dalším možným způsobem detekce ozbrojeného útočníka je využití nové videoanalytické funkce systémů VSS, tzv. „detekce zbraně“. Na základě této funkce je systém VSS schopen analyzovat tvar zbraně a předat varovný signál na dohledové centrum nemocnice.

Obr. 3 – Tísňový hlásič SZ 3 s ochranou proti nechtěné aktivaci [40]

Jako optimální možnost umožňující rychlý zásah příslušníky FOs se jeví využívání TH, protože poplachový stav není zapotřebí ověřovat a není nutné dispečerovi předávat další informace o poplachu, jelikož jsou součástí samotné poplachové zprávy. Jako nejméně příznivá varianta z pohledu rychlosti zásahu příslušníky FOs se jeví využívání tísňových linek (112 nebo 158). U této varianty dochází při předávání informací k citelnější časové prodlevě, jelikož IZS tvoří mezi oznamovatelem a dispečerem dohledového centra prostředníka. Naopak pokud bychom se zaměřili na potřebu zásahu jednotek IZS, tak se jako ideální varianta jeví především využití tísňových linek. Zde můžeme pociťovat znatelný časový rozdíl v příjezdu jednotek IZS oproti situaci, při níž by byl poplachový stav předán např. prostřednictvím vnitřních komunikačních klapek. Pokud některá z přítomných osob zvolí možnost využití vnitřních komunikačních klapek nebo tísňových linek, je potřeba v rozhovoru s operátorem sdělit minimálně tyto informace:

- počet útočníků;
- vzhled útočníka;
- kde se nachází nebo kde byl naposledy spatřen;
- směr pohybu útočníka;
- informace o obětech, rukojmích.

V praxi lze očekávat, že zásah proti útočníkovi bude proveden útvarem rychlého nasazení, proto je nutné se ve všech případech zaměřit na okamžité informování IZS. Níže na Obr. 4 jsou znázorněny posloupnosti událostí, které jsou součástí předávání poplachové informace na dohledové centrum výše uvedenými postupy. V reálné situaci se čas samotného zásahu jednotek IZS a FOs bude samozřejmě odvíjet od vzdálenosti jednotek IZS, rychlosti předávání informace, velikosti dotčeného objektu apod., proto je potřebné brát Obr. 4 pouze orientačně.



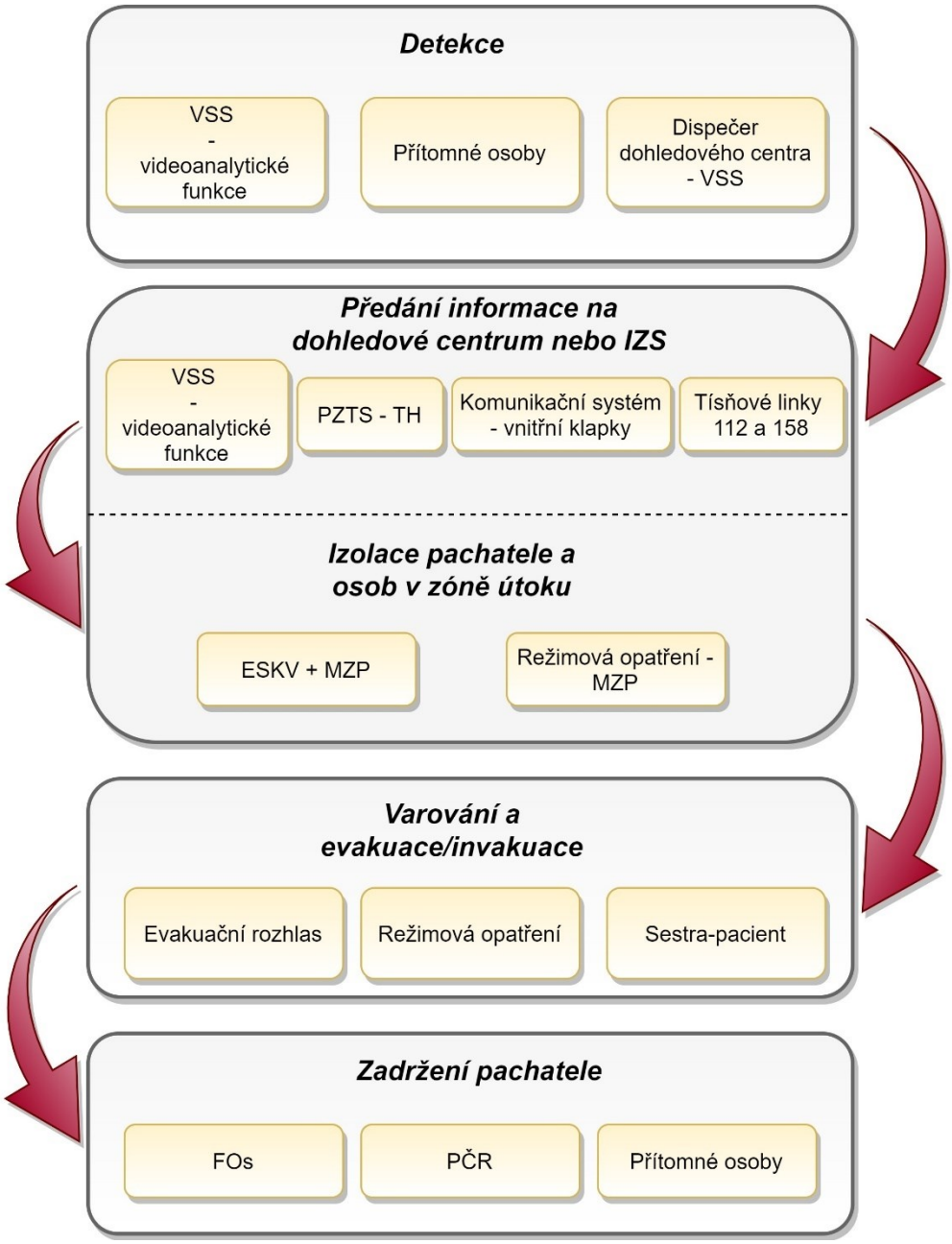
Obr. 4 – Posloupnost událostí při předávání informace o poplachu [autor]

Pro zajištění funkčnosti navrženého scénáře je potřeba objekt nemocnice v systémech PZTS a ESKV rozdělit do několika podsystémů – zón. Samostatné zóny budou tvořit jednotlivá oddělení. Další podsystémy by měly tvořit všechny průchody mezi objekty, aby bylo možné omezit pohyb pachatele mezi dalšími objekty areálu. Po přijetí a případném ověření poplachové informace o ozbrojeném útoku je potřeba neprodleně uzavřít prostor, ve kterém se ozbrojený útočník nachází (dále je v diplomové práci využíván termín zóna útoku), aby se zamezilo jeho úniku a ohrožování dalších osob v areálu nemocnice. Uzamčení vstupů bude provedeno automaticky elektromechanickými zámky s inverzní funkcí. Tímto opatřením bude znemožněn vstup do zóny útoku dalším neoprávněným osobám. Pokud budou v zóně útoku dveře, které vedou pouze vnějšího prostoru a fungují jako úniková trasa, lze tyto dveře ponechat otevřené pouze z vnitřní strany. Zónu útoku je vhodné tzv. „zakonzervovat“ systémem PZTS, kdy se automaticky zastřeží podsystém tvořící všechny vstupy vedoucí do zóny útoku. V případě násilného

otevření zastřeženého vstupu v zóně útoku bude dispečer dohledového centra informován, jakými dveřmi a kterým směrem útočník ze zóny útoku unikl. Aby mohl být podsystém se vstupy do zóny útoku zastřežen, je nutné zajistit, že tyto vstupy budou pokaždé uzavřeny např. dveřními samozavírači.

Po předání informace o útočníkovi na dohledové centrum musí být neprodleně zajištěna ochrana přítomných osob a izolace pachatele prostřednictvím režimových opatření, MZP a systémem ESKV. Varování osob o vzniklé situaci bude zajištěno prostřednictvím evakuačního rozhlasu spuštěním předem nadefinované digitální zprávy (viz Tab. 7). Personál nemocnice musí být na tyto digitální zprávy důkladně proškolen, aby mohla být neprodleně aplikována vhodná režimová opatření. Řízení invakuace/evakuace osob bude následně zajištěno právě personálem nemocnice a pracovníky FOs. Součástí Přílohy č. 6 je vytvořený metodický návod, jak postupovat při ozbrojeném útoku. Zjednodušené schéma postupu při útoku ozbrojeným pachatelem je znázorněno na Obr. 5.

Dalším možným řešením, jak varovat personál nemocnice o ozbrojeném útoku, je propojit systém PZTS spolu se systémem sestra-pacient. Na komponenty systému sestra-pacient, které jsou vyvedeny k personálu nemocnice, budou přenášeny poplachové informace z TH. Personál obdrží v tichosti informaci o nebezpečném útočníkovi, včetně informace o jeho lokalizaci. Tím se může personál rozhodnout, zda je vhodnější provést evakuaci nebo invakuaci přítomných osob.



Obr. 5 – Schéma postupu při útoku ozbrojeným útočníkem [autor]

Ambulantní péče

Jednotlivá ambulantní oddělení budou tvořit samostatné zóny (příkladný návrh zón je uveden na Obr. 7). Pokud se bude jednat o oddělení větších rozměrů a předpokládá se zde kumulace velkého množství osob, je doporučeno oddělení rozdělit na samostatné menší zóny. V každé zóně bude vytipována místnost, která bude sloužit k improvizovanému ukrytí. Všechny dveře sloužící ke vstupu/výstupu do zóny je vhodné opatřit elektromechanickými zámky s inverzní funkcí. Tyto zámky budou vzdáleně ovládány buď

automaticky, nebo manuálně z dohledového centra operátorem. Všechny místnosti v jednotlivých zónách musí být zařazeny do skupiny veřejných nebo neveřejných prostor. Veřejné prostory je vhodné vybavit uzamykacím systémem s kováním typu klika-klika, které budou opatřeny na vnitřní straně integrovaným knoflíkem v cylindrické vložce pro snadné zamknutí dveří v případě nutného lock-downu neboli „**uzamčení se**“. Neveřejné prostory je doporučeno zajistit mechanickými samozamykacími zámky s kováním typu knoflík-klika.

Jestliže by útočník započal svůj útok v čekárně ambulantního oddělení, je potřeba informaci o útoku ihned předat na dohledové centrum způsoby uvedenými na Obr. 4. Každá poplachová informace musí být následně dispečerem v nadstavbovém softwaru potvrzena do předem nastaveného časového limitu. Pokud bude aplikována varianta využívající TH, bude zóna útoku, ze které poplachový signál přišel, automaticky uzavřena za pomoci elektromechanických zámků. Pokud bude poplachový stav předán na dohledové centrum systémem VSS, vnitřními komunikačními klapkami nebo skrze tísňové linky, bude zóna útoku uzamčena vzdáleně dispečerem. V případě, že nebude dispečerem poplachová informace v nadstavbovém softwaru potvrzena, bude zóna uzavřena automaticky. Zámky je třeba nastavit tak, aby v případě běžného provozu byly obě strany volně průchozí (beznapěťový stav). Obě kliky zámků budou opět funkční po přiložení ovládacího zařízení ESKV např. čtečky s požadovaným přístupovým právem. Přístupové právo v této situaci musí mít pouze pracovníci FOs, kteří budou do zóny útoku vstupovat s příslušníky PČR. Po předání poplachové zprávy budou dispečerovi na monitorech dohledového centra zobrazeny živé pohledy z kamer, které jsou v zóně útoku instalovány.

V případě, že útočník zbraní pouze vyhrožuje, není doporučeno v objektu spouštět žádné digitální zprávy skrze evakuační rozhlas, aby nedošlo k jeho rozrušení. Nemocniční personál využije deeskalační metody, které byly popsány v kapitole 7.1. Dispečer dohledového centra musí nepřetržitě sledovat aktuální situaci v zóně útoku a v případě započetí útoku dispečer prostřednictvím evakuačního rozhlasu spustí v objektech digitální zprávu „*Kód 1*“ představující úmyslný útok (viz Tab. 7). Je doporučeno, aby zaměstnanci po vyhlášení zprávy ihned zahájili invakuaci všech přítomných osob a provedou tzv. lock-down. Invakuaci provedou především osoby přítomné v zóně útoku. Hlavním cílem procedury je se dostat z ohrožených prostor a vyhledat vhodnou místnost pro ukrytí. K možnému ukrytí budou sloužit zejména vytipované místnosti improvizovaného ukrytí.

V místnostech se uzamknou, popřípadě zatarasí vstupní dveře nábytkem, zhasnou, vypnou zvonění na svých mobilních telefonech a vyčkají na další pokyny PČR. Za předpokladu, že nebude možné místnost improvizovaného ukrytí využít, lze využít i jiný prostor, který bude v co nejvyšší míře splňovat níže uvedená kritéria:

- zděná místnost (bez skleněných výplní);
- uzamykatelné dveře;
- možnost úniku z místnosti (např. oknem v 1.NP);
- vybavená komunikačními systémy.

Pokud se ohroženým osobám nepodaří ukrýt v některé z místností, musí být jimi aplikován globální koncept cesty k přežití „**utíkej – schovej se – bojuj**“. Ve zbylé části objektu provede uzamknutí zón proškolený personál nebo vzdáleně dispečer dohledového centra. Všechny vstupy do zóny, která není zónou útoku, bude moci uzavřít personál jedním tlačítkem, které bude umístěno např. na sesterně nebo v ordinaci lékaře. Tlačítko bude funkční pouze v případě vyhlášení poplachu s ozbrojeným pachatelem. Součástí tlačítka bude světelná signalizace upozorňující na možnost využití tlačítka.

Pro ochranu lidí v zóně útoku je vhodné prostory vybavit zamlžovacím systémem s dostatečně rychlým zamlžením (příkladné zamlžení prostoru je znázorněno na Obr. 6). Tím budou mít osoby v zóně možnost zabránit pachateli v útoku, popřípadě se mohou v mlze ukrýt. Nespornou výhodou zamlžení prostoru je snížení orientace pachatele, a tím je snížená možnost pokračování v útoku. Pokud se bude jednat o oddělení, kde se vyskytují převážně čekárny s malou kapacitou, bude vhodnější zamlžovací systém instalovat na chodbě oddělení. Zamlžovací systém bude oprávněn spustit pouze dispečer dohledového centra v závislosti na průběhu situace. V případě jeho použití bude v objektu automaticky vyhlášena digitální zpráva *„V objektu byla spuštěna bezpečnostní mlha*“. Na základě instalace zamlžovacího systému bude potřeba zvážit vybavení těchto prostor hlásiči EPS, kdy není vhodné se zamlžovacím systémem instalovat opticko-kouřové hlásiče kouře.

Obr. 6 – Příklad použití zamlžovacího systému v obchodním domě [24]

Obr. 7 znázorňuje typovou situaci, kdy se ozbrojený útočník dostal na jedno z ambulantních oddělení. Při zpozorování útočníka v čekárně byl personálem aktivován tísňový hlásič. Poplachový signál byl předán na dohledové centrum, kdy bez nutnosti ověření dispečerem dojde k automatickému uzamčení vstupních dveří do zóny útoku (červeně označené dveře). V objektu nemocnice byla po započetí útoku dispečerem skrze evakuační rozhlas spuštěna digitální zpráva „*Kód 1*“. Personál nemocnice se na základě digitální zprávy uzamkl v jednotlivých místnostech (žlutě označené dveře), popřípadě pomohl s ukrytím dalším přítomným osobám. Osoby, které se pohybovaly na chodbě se drželi pravidla „utíkej – schovej se – bojuj“. Pro ukrytí využily místnost improvizovaného ukrytí (žlutě označená místnost). Osoby, které byly mimo uzamčené zóny využily evakuační cesty. Na dohledovém centru byly zobrazeny živé pohledy z kamer K1 a K2. Dispečer ve vhodný okamžik spustil zamlžovací systém, který byl instalován v prostoru chodby, čímž byla orientační schopnost útočníka snížena na minimum. Útočník byl následně zadržen příslušníky PČR se součinností FOs, která měla přiřazena práva otevírat tyto prostory v případě této MU. Ostatní zóny zůstaly uzamčeny až do vyhlášení klidové situace „*Kód 4*“.

Obr. 7 – Modelová situace s ozbrojeným útočníkem v ambulanci [autor]

Lůžkové oddělení

Na lůžkovém oddělení je zpočátku potřeba zavést přísná režimová opatření. Vstupy na jednotlivá lůžková oddělení by měly být trvale uzamčeny. Osoba, která bude požadovat vstup na oddělení, musí být prověřena zdravotní sestrou na sesterně např. za pomoci interkomu. Osoba vyžadující vstup na oddělení musí uvést své celé jméno, jméno navštěvované osoby a vztah k této osobě. Vstupy na lůžková oddělení budou vybaveny elektromechanickými zámky s inverzní funkcí. Ty budou v běžném provozu oboustranně neprůchozí. Pro odchod bude návštěva opět puštěna personálem oddělení, aby se na oddělení nedostala neoprávněná osoba. Pro přivolání pomoci a předání poplachové informace musí být v každém pokoji instalovány TH, které budou dosažitelné z každého lůžka. Systém sestra-pacient je nutné oddělit od TH v systémech PZTS. Dispečer dohledového centra musí získávat pouze informace týkající se bezpečnostních incidentů. Informace ohledně zdravotních problémů pacientů musí jít pouze na zdravotnický personál daného oddělení. Lékařské pokoje a vyšetřovací místnosti je doporučeno zajistit mechanickými zámky s dostatečnou mechanickou odolností a kováním typu knoflík-klika. Veškeré pokoje je potřeba vybavit evakuačním rozhlasem pro ozvučení a zajištění přenosu poplachové zprávy.

Jestliže by útočník započal svůj útok na lůžkovém oddělení, je potřeba informaci o útoku neprodleně předat na dohledové centrum způsoby uvedenými na Obr. 4. Rychlou a spolehlivou variantou předání informace o ozbrojeném útočníkovi je využití TH v systému PZTS. Po potvrzení poplachové situace bude ihned zakázána možnost otevírání vstupních dveří na dané lůžkové oddělení ze sesterny. Za pomoci evakuačního rozhlasu bude po započetí útoku na sesternách, lékařských pracovištích a chodbách spuštěna digitální zpráva „*Kód 1*“. Proškolený personál zahájí invakuaci do jakéhokoli z uzamykatelných prostorů. Pokud to bude situace umožňovat, vypomůže dalším osobám se ukrýt a uzamknout. Na lůžkových pokojích pro pacienty bude spuštěna digitální zpráva „*Uzamkněte, prosím, své pokoje a nevycházejte*“, proto je nutné uzamykací systém lůžkových pokojů opatřit cylindrickou vložkou s integrovaným knoflíkem na vnitřní straně. Na monitorech dohledového centra budou dispečerům zobrazeny živé pohledy z kamer v zóně útoku. Do zóny útoku bude mít opět přístup pouze osoba s přiděleným oprávněním v případě vzniku této MU (pouze FOs).

Jelikož na lůžkovém oddělení mohou být hospitalizováni pacienti s omezenou mobilitou, je pro jejich hospitalizaci vhodné na každém lůžkovém oddělení vyčlenit několik lůžkových pokojů. Vstupní dveře do těchto pokojů budou vybaveny elektromechanickými zámky s inverzní funkcí. V klidovém stavu budou obě kliky kování aktivní a bude zajištěn volný vstup do těchto prostor. Zámky bude možné vzdáleně ovládat ze sesterny nebo dispečerem dohledového centra. V případě, že bude na lůžkovém oddělení zpozorován ozbrojený pachatel, sestra nebo dispečer tyto pokoje vzdáleně uzamkne.

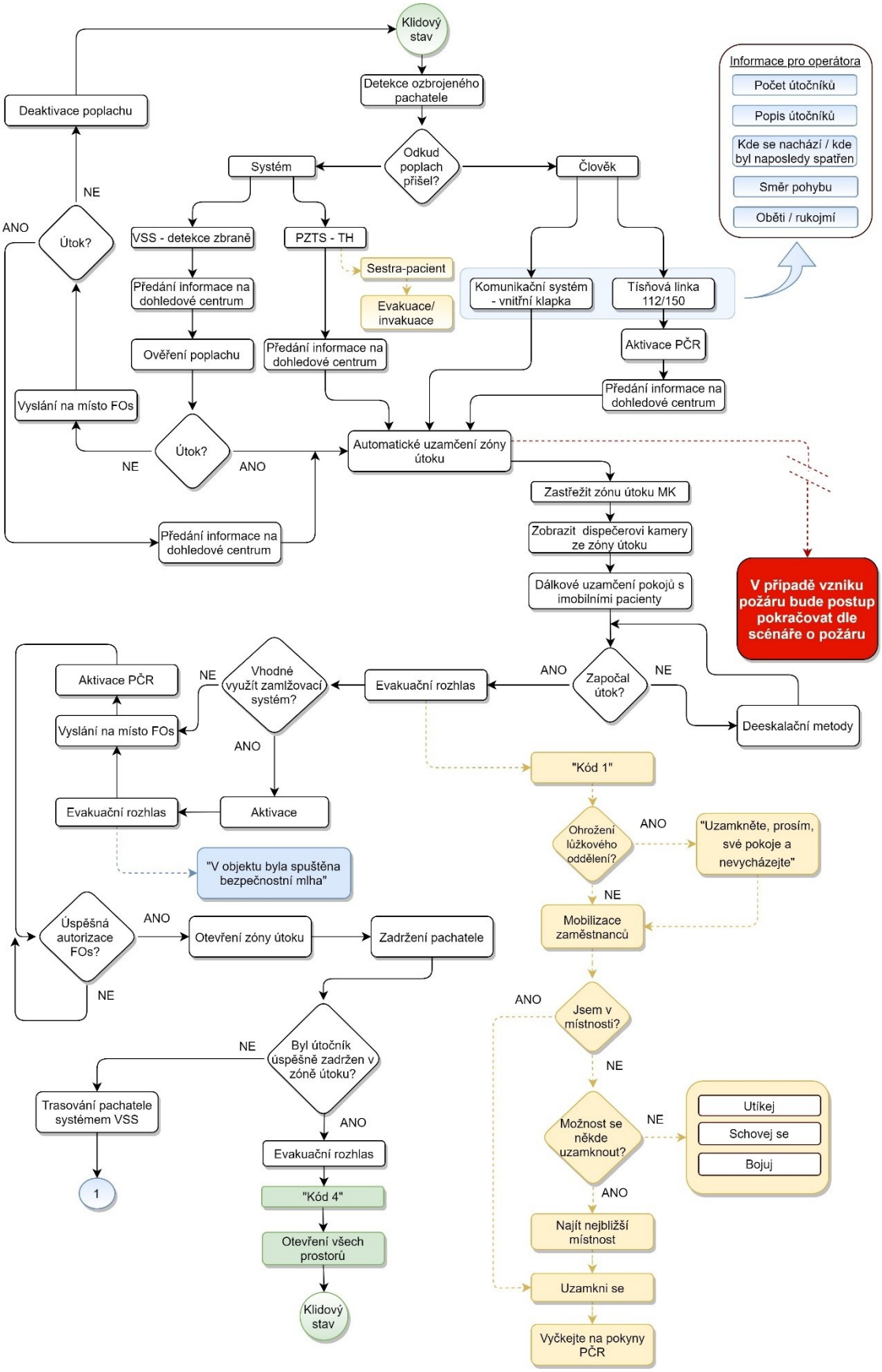
Na Obr. 8 je znázorněna modelová situace, kdy se ozbrojený pachatel dostal na sesternu jednoho z lůžkových oddělení. Jedna ze zdravotních sester v místnosti aktivovala TH, který předal informaci o útočníkovi dispečerovi na dohledové centrum. Prostřednictvím evakuačního rozhlasu byla dispečerem spuštěna v celém objektu digitální zpráva „*Kód 1*“. Na jednotlivých lůžkových pokojích se skrze evakuační rozhlas spustila hláška „*Uzamkněte, prosím, své pokoje a nevycházejte*“. Pacienti, personál a návštěvníci reagují okamžitě, uzamknou své pokoje, schovají se a chovají se tiše. Na dohledovém centru se dispečerovi zobrazily pohledy ze všech kamer v zóně útoku, v tomto případě kamery s označením K1, K2, K3 a K4. Azurově označená místnost, určená pro imobilní pacienty, je vzdáleně uzamčena dispečerem dohledového centra. Osoba, která se nachází na chodbě a snaží se ukrýt a využije místnost improvizovaného ukrytí, kde se uzamkne a vyčká na pokyny FOs nebo PČR.

Obr. 8 – Modelová situace s ozbrojeným útočníkem na lůžkovém oddělení [autor]

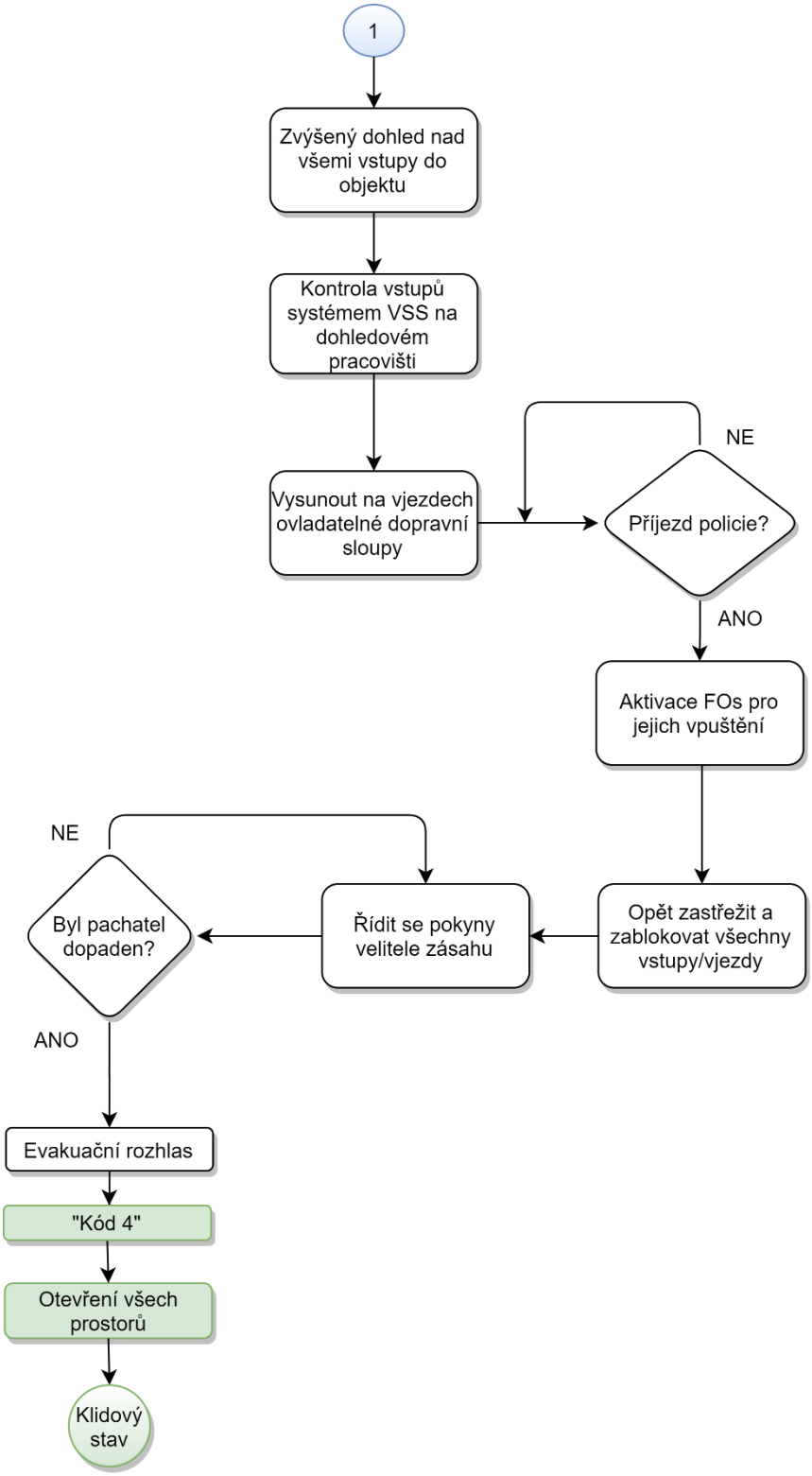
Požár v případě ozbrojeného útoku

V rámci uzamykání jednotlivých místností je nutné vzít v úvahu systém EPS a možnost vzniku požáru v uzavřené zóně. Systém EPS musí být trvale v provozu a musí být zajištěna jeho stálá kontrola (na Obr. 9 se jedná o červeně vyznačenou část). V případě, že budou jednotlivé zóny uzavřeny prostřednictvím systému ESKV, ale v objektu dojde ke vzniku požáru, je nutné uzavřené místnosti opět otevřít, aby byla umožněna evakuace přítomných osob v budově. Při návrhu uzavíraní jednotlivých zón útoku je proto třeba dodržovat požadavky uvedené v požárně bezpečnostním řešení stavby. Ovládání dveří systémem EPS musí mít vyšší prioritu než ostatní systémy. Kombinace těchto systémů pro ovládání zámků je možná prostřednictvím reléových kontaktů pro zajištění galvanického oddělení jednotlivých systémů. Priority různých systémů je poté potřeba nastavit prostřednictvím vhodného zapojení kontaktů. V případě vzniku požáru bude do každého prostoru prostřednictvím evakuačního rozhlasu spuštěna digitální zpráva „*Kód 3*“.

Na Obr. 9 a Obr. 10 je vytvořen obecný scénář popisující možný způsob řešení situace při zpozorování a útoku ozbrojeným pachatelem. Čárkovaně označené postupy budou probíhat paralelně s dalšími opatřeními.



Obr. 9 – Vývojový diagram postupu při ozbrojeném útoku (část 1) [autor]

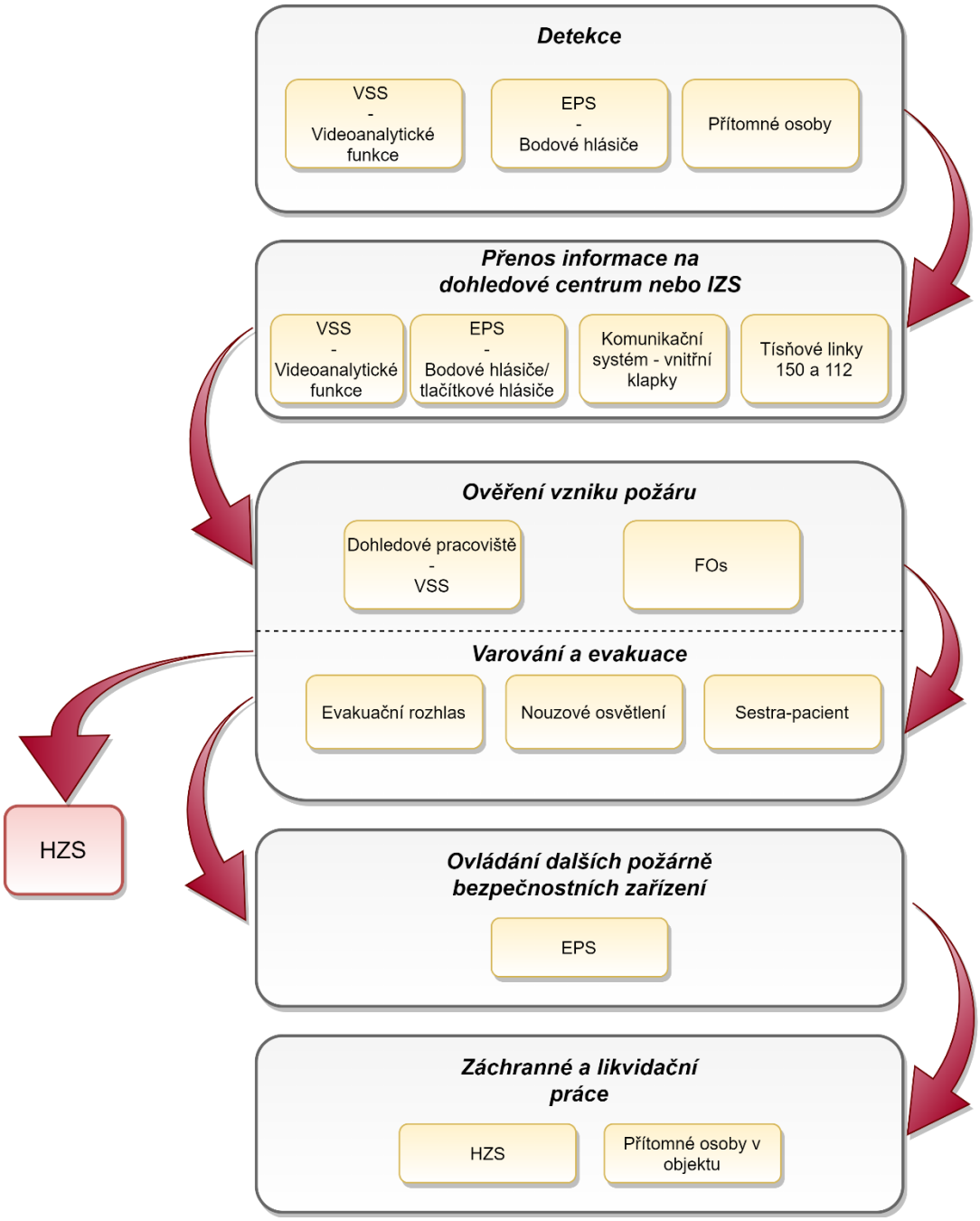


Obr. 10 – Vývojový diagram postupu při ozbrojeném útoku (část 2) [autor]

7.3 Požáry

Vytvořený bezpečnostní scénář popisuje postup aplikování jednotlivých funkcí instalovaných STO, systému EPS a dalších režimových opatření umožňující rychlejší detekci, ověření a evakuaci osob v případě vzniku požáru v objektech nemocnic. Požár může být založen úmyslně (žhářský útok), může vzniknout z nedbalosti, popřípadě může být jeho iniciátorem technická závada. Základní postupy musí vycházet ze zpracovaných požárně-poplachových směrnic a evakuačních plánů. Diplomová práce se nezabývá požadavky na rozsah a způsob instalace systému EPS, jelikož tyto požadavky jsou důkladně popsány v platných právních a normativních předpisech týkajících se PBZ.

Pro detekci a následnou signalizaci požáru bude využíván primárně systém EPS. Jako sekundární systém pro detekci požáru je doporučováno využívat pokročilé videoanalytické funkce systému VSS. Objekty nemocnic jsou v rámci zvládání požáru kritické především v tom, že je zde komplikovaná evakuace pacientů s omezenou mobilitou. Pro efektivní zvládnutí situace je proto nezbytné zajistit včasnou detekci a ohlášení požáru. V případě, že bude v objektu detekován požár, musí být poplachový stav neprodleně předán na dohledové centrum, které bude zároveň splňovat funkci ohlašovny požáru. Zde dispečeři zajistí ověření poplachové informace. Varování a evakuace osob v areálu bude řízena především evakuačním rozhlasem a nouzovým osvětlením. Na základě varování je nezbytnost zajistit rychlou a správnou reakci personálu. Automatické ovládání dalších PBZ, jako je např. ZOTK, SHZ, požární dveře, požární klapky apod., bude zajištěno pouze prostřednictvím systému EPS. Zjednodušené schéma výše popsaného postupu je zobrazeno na Obr. 11.



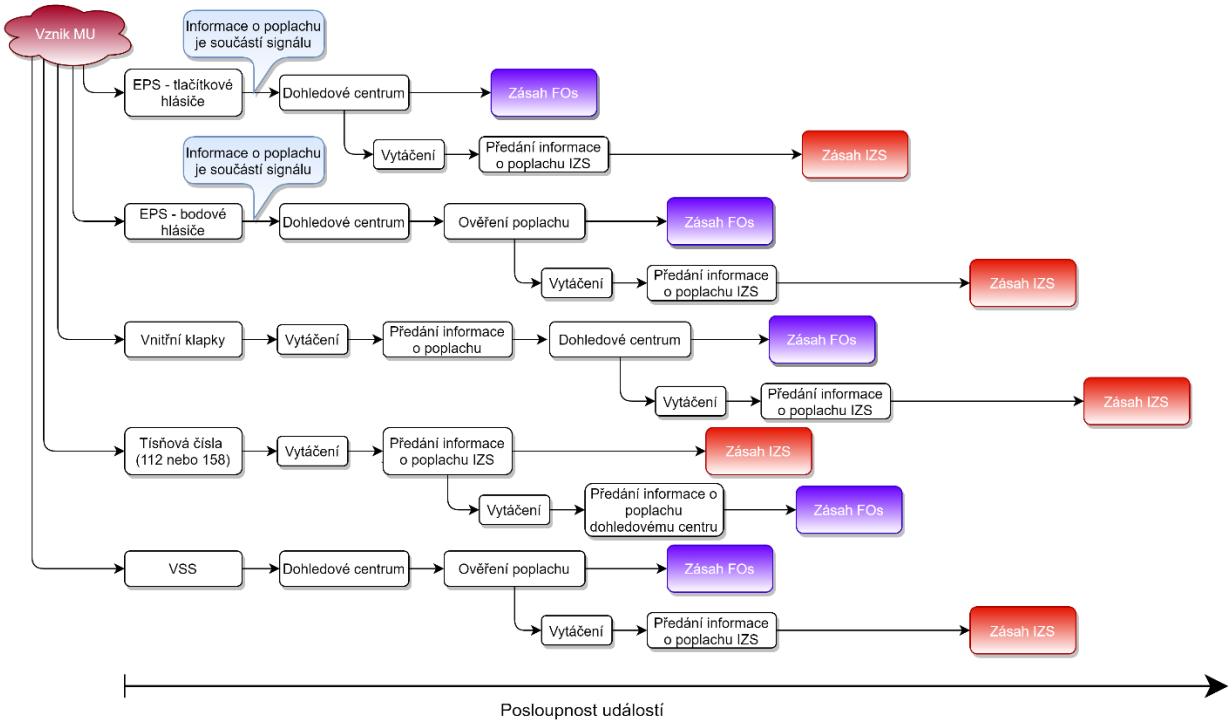
Obr. 11 – Schéma postupu zvládnutí požáru [autor]

Pro dosažení vyšší efektivity systému EPS je doporučeno systém integrovat do nadstavbového softwaru na dohledovém centru nemocnice. Připojení k nadstavbovému softwaru nabídne propojení s dalšími připojenými systémy, především se systémem VSS. Zde bude nastavena logická závislost, že v případě vzniku požáru budou dispečerovi na dohledovém centru zobrazeny pohledy z nejblíže instalovaných kamer. Obsluha

dohledového centra tak získá větší přehled o místě vzniku požáru. Informace o požáru může být na dohledové centrum předána několika způsoby:

- systémem EPS;
    - bodové hlásiče;
    - tlačítkové hlásiče;
    - ostatní typy (např. nasávací systémy);
- systémem VSS (videoanalytické funkce);
- komunikační prostředky nemocnice (vnitřní klapky);
- informování tísňové linky (tel. číslo: 112, 150).

V případě zpozorování požáru je nejdůležitější zachovat klid a co nejrychleji vyhlásit požární poplach. Optimální variantou pro rychlý zásah FOs je využití tlačítkového hlásiče systému EPS. Jestliže požár zpozoruje někdo z personálu nemocnice, je další možností využití nemocničních komunikačních systémů (vnitřní klapky). Tento způsob předání poplachové informace může mít v praxi větší časovou prodlevu z důvodu vytáčení tel. čísla, popisování situace, určení místa zásahu apod. Nicméně v případě požáru je potřeba zajistit v co nejkratším čase především zásah HZS. Z tohoto pohledu se jako optimální varianta jeví využití tísňových čísel 150, eventuelně 112. V případě, že IZS dostane hlášení o vzniku požáru v areálu nemocnice, je kromě vyslání jednotek na místo požáru důležité informovat dohledové centrum nemocnice, aby mohla být především zahájená okamžitá evakuace osob. Na Obr. 12 je znázorněna posloupnost událostí, které je potřeba provést při předávání poplachové informace ohledně požáru dle výše uvedených možností.



Obr. 12 – Posloupnost událostí při předávání informace o požáru [autor]

Jestliže poplachový stav přijde z tlačítkového hlásiče, bude dle normativních požadavků bez nutnosti jeho ověření vyhlášen poplach a obsluha dohledového centra zajistí svolání HZS na místo požáru. V případě, že požár bude detekován bodovými hlásiči nebo jiným typem hlásičů, jako je např. lineární hlásič nebo nasávací jednotky, bude potřeba zajistit ověření požárního poplachu pracovníky FOs. Pracovníci FOs ověří poplach buď tím, že místo požáru sami navštíví nebo pokud to bude rozsah systému VSS umožňovat, ověří požár za pomocí instalovaných kamer z dohledového centra. Nadstavbový software proto automaticky pro zkrácení reakční doby obsluhy zprostředkuje pohledy kamer z místa incidentu. Jestliže se v prostoru nebude kamerový systém nacházet, nadstavba zprostředkuje záběry z nejbližšího místa. Potřeba ověření bude taktéž zapotřebí, pokud poplachový stav přijde ze systému VSS na základě využití videoanalytické funkce. Jestliže poplachová informace o požáru přijde na dohledové centrum ze systémů EPS a VSS zároveň, bude bez nutnosti ověření potvrzen poplachový stav a na místo budou svolány jednotky HZS. Dále bude v nadstavbovém softwaru přednastavena možnost vytvoření výjezdového lístku, který bude následně automaticky zaslán předem určené jednotce HZS nebo bude předán veliteli zásahu při příjezdu jednotek IZS. Výjezdový lístek si bude moct dispečer vytisknout pro další potřeby. Lístek by měl především obsahovat následující informace:

- označení budovy, patra a místnosti s požárem;
- označení budovy na situační mapě;
- označení hydrantů a přípojných míst polostabilních hasících zařízení apod.;
- označení vjezdů do areálu;
- označení vstupů do budovy;
- informace, co se v místnosti nachází;
- označení hlásiče v dispozičním výkresu;
- typ a označení hlásiče, ze kterého poplach přišel.

Objekty nemocnic je doporučeno vybavit adresnými bodovými hlásiči s integrovanou sirénou a majákem. Tyto hlásiče budou v případě detekování požáru ihned vyhlašovat lokální požární poplach prostřednictvím integrované sirény, a to ještě před ověřením poplachového stavu na dohledovém centru. Tímto opatřením budou osoby vyskytující se v blízkosti ohniska požáru dříve informovány, čímž může zajištěna rychlejší evakuace osob z ohrožených prostor.

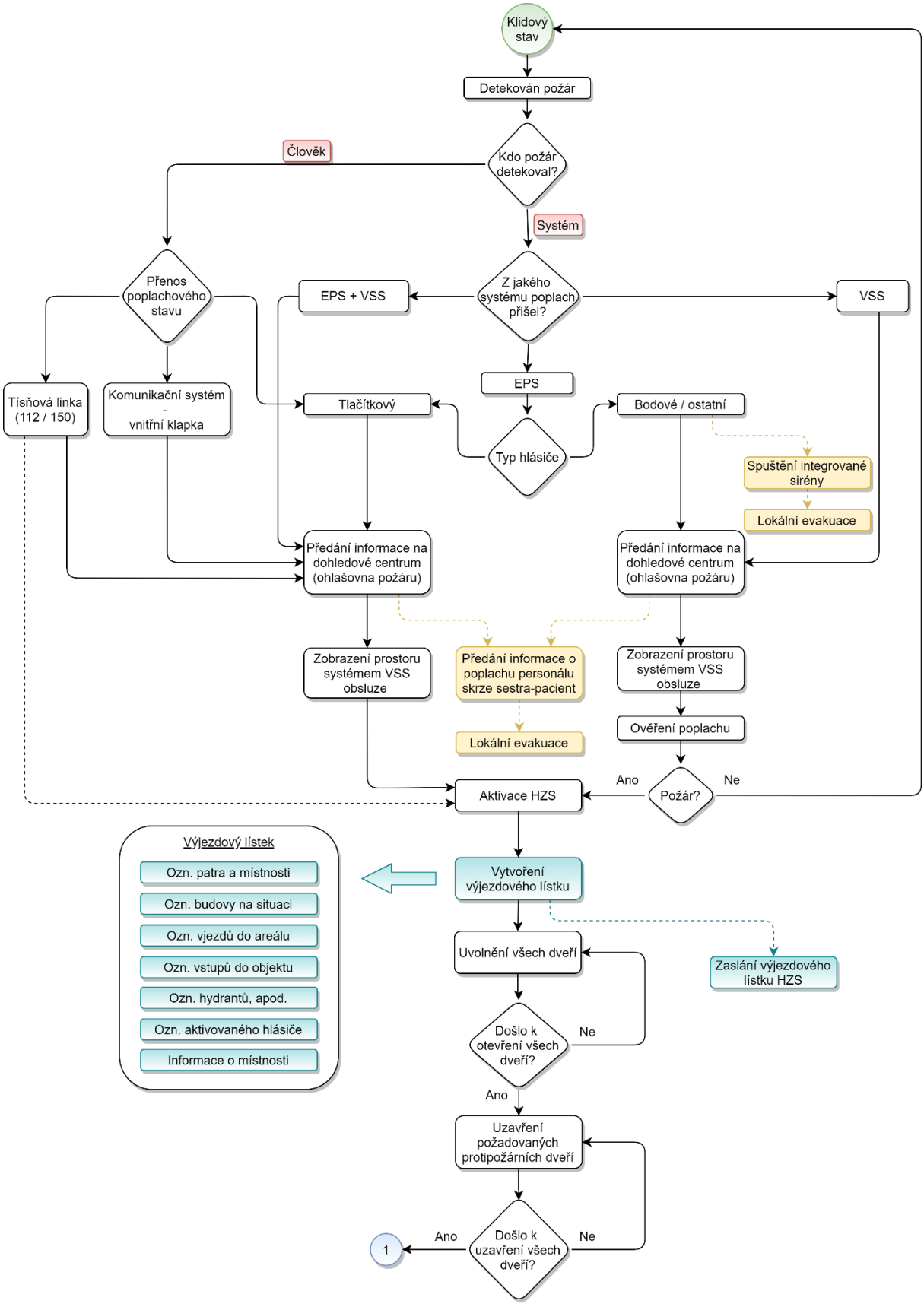
Jestliže bude požár dispečerem ověřen a potvrzen, bude vyhlášena skrze evakuační rozhlas přednastavená digitální zpráva „*Kód 3*“. Pokud to situace bude umožňovat, je možné se pokusit o zvládnutí zdolání požáru vlastními silami. Proškolený personál na základě digitální zprávy ihned započne evakuaci přítomných osob. Při evakuaci je nutné vnímat nastalou situaci pro možnost vzniku dalšího nebezpečí (např. výbuch nebo v případě žhářského útoku může útočník pokračovat v útoku). Pověřený personál na lůžkovém oddělení zajistí evakuaci všech mobilních i imobilních pacientů. Před opuštěním lůžkového oddělení je nezbytné zkontrolovat aktuální stav, zda v pokojích nezůstal některý z pacientů. V případě, že na pokoji zůstala osoba, kterou není možné z určitých důvodů evakuovat, personál neprodleně předá informaci kterémukoli členovi jednotek IZS.

Dalším možným řešením varování personálu nemocnice o požáru je propojení systému EPS spolu se systémem sestra-pacient. Komponenty systému sestra-pacient bývají vybaveny především lůžkové pokoje, sesterny, lékařské pokoje nebo samotný personál, který je vybaven osobními pagery. Na komunikační zařízení personálu by bylo možné přenášet poplachové informace o vzniklém požáru přímo z ústředny EPS, kdy na koncových prvcích sestra-pacient by poplachová informace byla zasílána ve tvaru, v jakém je zasílána na ohlašovnu požáru. Tím by byl personál nemocnice informován jak o vzniku

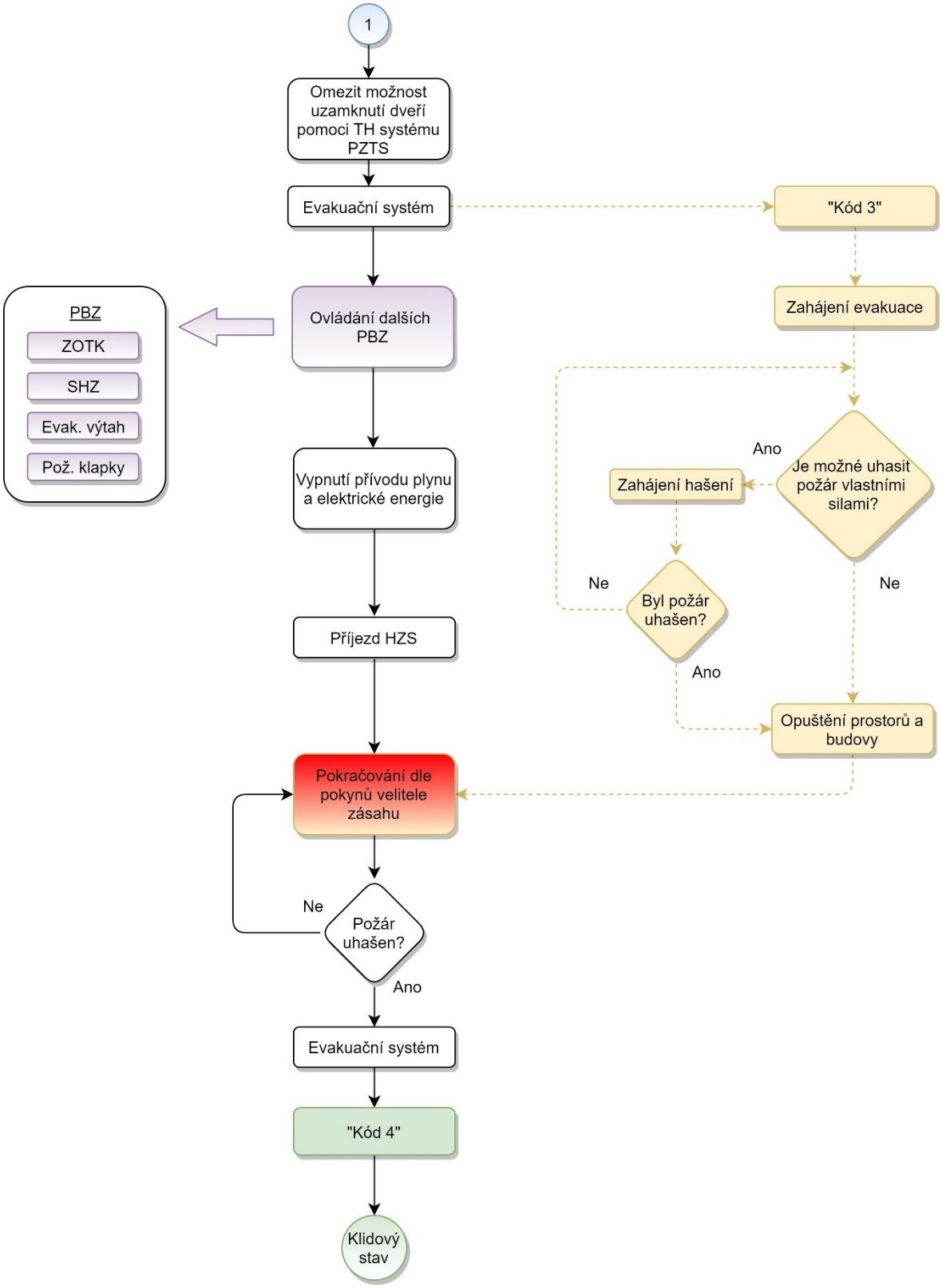
požáru, tak i o jeho lokalizaci. Zde je nutné upozornit, že zmíněné řešení nenahrazuje využívání evakuačního rozhlasu.

Pro zamezení šíření požáru mezi jednotlivými požárními úseky budou využívány protipožární dveře, které budou ovládány systémem EPS. Ovládání dveří systémem EPS musí mít nastavenou vyšší prioritu než systémy ESKV. Systém EPS také automaticky za pomoci ovládacích zařízení (relé) uzavře přívody plynu a elektrické energie. Při vzniku požáru je nutné, aby byly z funkce vyřazeny TH systému PZTS, které jsou schopny uzamknout dveře do prostorů (zóna ohrožení), kde se TH nachází.

Scénář postupu je zobrazen na Obr. 13 a Obr. 14.



Obr. 13 – Vývojový diagram postupu při vzniku požáru (část 1) [autor]



Obr. 14 – Vývojový diagram postupu při vzniku požáru (část 2) [autor]

Závěr

Diplomová práce měla za cíl zpracovat pro nemocniční zařízení bezpečnostní scénáře, které budou popisovat posloupnost aplikování vybraných funkcí systémů technické ochrany, požární ochrany a dalších opticko-akustických systémů s návazností na uplatňování jednotlivých režimových opatření v případě vzniku mimořádné události tak, aby bylo zajištěno efektivní řešení vzniklé situace.

V úvodu práce je provedena rešerše odborné literatury, provedených studií a technických norem související s problematikou bezpečnosti zdravotnických zařízení. Informace z těchto zdrojů byly následně využity při zpracování diplomové práce. Teoretická část se zabývá stručným popisem zdravotnických zařízení, včetně jejich kategorizace. Následující část díla je zaměřena pouze na nemocniční zařízení, ve kterých se na základě jejich charakteristických vlastností předpokládá kritický dopad na funkčnost s ohledem na vznik mimořádné události. Na základě provedeného průzkumu situace ohledně vzniklých bezpečnostních incidentů v nemocničních zařízeních a na základě posouzení rizik byly zpracovány jednotlivé bezpečnostní scénáře zaměřující se na způsob řešení verbálního a fyzického napadení, ozbrojeného útoku a požáru. Práce je zaměřena na oddělení poskytující ambulantní a lůžkovou péči, která se s ohledem na charakter provozu mohou stát atraktivním cílem pro potenciálního útočníka a lze zde předpokládat kritický dopad na možnost poskytování nezbytné zdravotnické péče v závislosti na vznik mimořádné události.

Navržené bezpečnostní scénáře pro vybrané mimořádné události mohou v rámci projekčních a koordinačních činností sloužit jako doporučený nástroj pro navrhování a efektivní nastavení bezpečnostních opatření. Důležitým krokem vedoucím ke zvýšení ochrany posuzovaných objektů je především zřízení jednotného, digitalizovaného dohledového centra v areálu nemocnice, kde budou do zvoleného nadstavbového softwaru integrovány jednotlivé systémy technické a požární ochrany, včetně dalších obvykle využívaných systémů. Nepostradatelným krokem k zajištění požadované míry bezpečnosti je nastavení vhodných režimových opatření. Na tato opatření je nezbytné opakovaně zřizovat školení personálu, včetně neustálé kontroly jejich aplikovatelnosti.

Na závěr práce je nutné konstatovat, že se jedná o obecné scénáře, které je potřeba přizpůsobit požadavkům konkrétního areálu nemocnice. V nemocnicích jsou často zřizována oddělení, která jsou svým způsobem provozování odlišitelná od ostatních. Jako

příklad lze uvést např. dětská nebo psychiatrická oddělení, která s ohledem na typ pacientů fungují ve zvláštním režimu. Proto je samotné řešení bezpečnosti doporučeno pokaždé projednat s odpovědnými interními zaměstnanci jednotlivých oddělení a následně také s orgány vykonávajícími státní požární dozor.

Celkově lze v díle zpozorovat potenciál dalšího rozvoje, a to především v dopracování jednotlivých scénářů na další nemocniční oddělení nebo na další mimořádné události. Následně je možné zpracovat návrh integrace všech nemocnic na jedno centralizované dohledové centrum, které by mohlo zajišťovat zejména kontrolu odezvy dispečerů na poplachové stavy v dílčích dohledových centrech.

Seznam použité literatury

[1] AHASOFT. Call centrum operátor ploché vektorové ikony — Stocková ilustrace. *DEPOSITPHOTOS* [online]. 2017 [cit. 2021-03-21]. Dostupné z: https://cz.depositphotos.com/143787351/stock-illustration-call-center-operator-flat-vector.html

[2] ART PB 102 PANIC: Tísňový hlásič s pamětí aktivace. *DSTECHNIK* [online]. Marten & Louis, spol. s r.o. [cit. 2021-03-21]. Dostupné z: https://www.dstechnik.cz/tisnovy-hlasic-s-pameti-aktivace-art-pb-102-panic-4288.html

[3] *Attacks on health care in the context of COVID-19* [online]. 2020 [cit. 2020-09-20]. Dostupné z: https://www.who.int/news-room/feature-stories/detail/attacks-on-health-care-in-the-context-of-covid-19

[4] Babiarczyk, B., Turbiarz, A., Tomagová, M., Zeleníková, R., Önler, E., and Sancho Cantus, D. (2020). Reporting of workplace violence towards nurses in 5 European countries – a cross-sectional study. International Journal of Occupational Medicine and Environmental Health, 33(3), pp.325-338. https://doi.org/10.13075/ijomeh.1896.01475

[5] *Bezpečnostní systémy: Speciální tísňové hlásiče* [online]. Ústí nad Labem, 2010 [cit. 2021-01-31]. Dostupné z: http://studijni-materialy.sseas.cz/bezpecnostni-systemy/specialni-tisnove-hlasice/

[6] CÁBOVÁ, Markéta. *Zhodnocení hospodaření vybraných nemocničních zařízení v Moravskoslezském kraji* [online]. Ostrava, 2018 [cit. 2020-08-30]. Dostupné z: https://dspace.vsb.cz/bitstream/handle/10084/132915/CAB0023_EKF_N6202_6202T055_2018.pdf?sequence=1. Diplomová práce. VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA. Vedoucí práce Ing. Ivana Vaňková, Ph.D.

[7] C4. *Dominus Millenium* [online]. [cit. 2020-09-08]. Dostupné z: http://www.millennium.dominus.cz/software/c4/

[8] Charakteristika, postavení, vznik a transformace fakultních nemocnic v ČR. *Asociace děkanů lékařských fakult ČR* [online]. [cit. 2021-04-07]. Dostupné z: https://dekanilf.cz/onewebmedia/Charakter_fakultni_nemocnice.pdf

[9] *DEFENDIT: Mechanické zábranné systémy* [online]. [cit. 2021-01-31]. Dostupné z: https://www.defendit.cz/technicke-zabezpeceni/mechanicke-zabranne-systemy/

[10] FRANC, Jan. DOROZUMÍVACÍ SYSTÉMY SESTRA - PACIENT. *Dahasl s.r.o.* [online]. 2018 [cit. 2021-02-19]. Dostupné z: https://www.dahasl.cz/dorozumivaci-systemy-sestra-pacient

[11] Evakuační rozhlas a veřejné ozvučení. *Honeywell - Fire and PA/VA Solutions* [online]. [cit. 2020-08-25]. Dostupné z: https://www.hls-czech.com/cs-cz/business/public-address-and-voice-alarm-systems

[12] FRYŠAR, Miroslav. *Bezpečnost pro manažery, podnikatele a politiky*. Praha: Public History ve spolupráci s Českou asociací bezpečnostních manažerů, c2006. ISBN isbn80-86445-22-4.

[13] F.S.C. BEZPEČNOSTNÍ PORADENSTVÍ, a.s., Vítkovická 1994/22, Ostrava, *ZVÝŠENÍ ZABEZPEČENÍ MĚKKÉHO CÍLE: Interní dokument*. 2020. Ostrava, 2020.

[14] HAVRÁNEK, Miroslav. SDĚLENÍ KRAJSKÉHO ŘEDITELSTVÍ POLICIE STŘEDOČESKÉHO KRAJE. *Město Jesenice* [online]. 2019 [cit. 2021-03-21]. Dostupné z: https://mujesenice.cz/sdeleni-krajskeho-reditelstvi-policie-stredoceskeho-kraje/d-4718

[15] HOLUBOVÁ, V. Předmět Ochrana objektů. (přednáška) Ostrava: VŠB – TUO, Fakulta bezpečnostního inženýrství, Letní semestr 2018.

[16] IP vs. analog. Jaký kamerový systém zvolit? *SECURITAS* [online]. [cit. 2020-09-03]. Dostupné z: https://www.securitas.cz/blog/bezpecnostni-technologie/ip-vs-analog.-jaky-kamerovy-system-zvolit/

[17] IVANKA, Ján. *Mechanické zábranné systémy* [online]. Zlín, 2014 [cit. 2020-09-01]. ISBN ISBN 978-80-7454-427–9. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/18575/Mechanicke_zabranne_systemy-obsah.pdf?sequence=2&isAllowed=y

[18] KALVACH, Zdeněk. *VYHODNOCENÍ OHROŽENOSTI MĚKKÉHO CÍLE: aneb co, kdy, kde a od koho vám hrozí* [online]. Praha, 2018, , 40 [cit. 2021-02-07]. Dostupné z: https://www.mvcr.cz/cthh/soubor/vyhodnoceni-ohrozenosti-mekkeho-cile.aspx

[19] Klíče nebo oční duhovka? Vstup do budov dnes chrání vysoce sofistikované systémy. *SECURITAS* [online]. [cit. 2020-08-27]. Dostupné z: https://www.securitas.cz/blog/bezpecnostni-technologie/klice-nebo-ocni-duhovka-vstup-do-budov-dnes-chrani-vysoce-sofistikovane-systemy/?fbclid=IwAR2BULaoX5i-0TOZUIAjirIZIl1l2FUPcLDAeUsm-nPYXgQA1MarOLTZcGc

[20] *Komunikační zařízení SESTRA – PACIENT* [online]. [cit. 2020-08-23]. Dostupné z: http://www.jiriknizek.cz/sluzby/sestra-pacient/

[21] Lůžková oddělení. *Nemocnice Vyškov: Příspěvková organizace* [online]. [cit. 2020-09-08]. Dostupné z: https://www.nemvy.cz/luzkova-oddeleni-s-ambulancemi

[22] Nemocnice. *Velký lékařský slovník* [online]. [cit. 2020-10-05]. Dostupné z: http://www.lekarske.slovniky.cz/pojem/nemocnice

[23] NĚMCOVÁ, Tereza. *Subjekty zajišťující nemocniční péči* [online]. Ostrava, 2010 [cit. 2021-02-19]. Dostupné z: https://dspace.vsb.cz/bitstream/handle/10084/80847/NEM267_EKF_B6202_6202R055_02_2010.pdf?sequence=1. Bakalářská práce. VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA. Vedoucí práce Ing. Blanka Mlčáková, Ph.D.

[24] NĚMEČEK, Petr. Zamlžovací systémy. *PROTECT* [online]. PROTECT Czech Republic, 2015 [cit. 2021-03-22]. Dostupné z: https://www.aktivni-zabezpeceni.cz/sluzby/zamlzovaci-systemy/

[25] Madeleine Estryn-Behar, Beatrice van der Heijden, Donatella Camerino, Clementine Fry, Olivier Le Nezet, Paul Maurice Conway, Hans-Martin Hasselhorn, the NEXT Study group, *Violence risks in nursing—results from the European 'NEXT' Study* [online]. Occupational Medicine, Květen 2008, 107-114 [cit. 2021-02-24]. Dostupné z: https://doi.org/10.1093/occmed/kqm142

[26] Maslowova pyramida potřeb. *Filozofie úspěchu* [online]. 2012 [cit. 2020-08-27]. Dostupné z: http://www.filosofie-uspechu.cz/jak-motivovat-zamestnance/

[27] *PERFETCED: Mechanické zábranné prostředky (MZP)* [online]. [cit. 2021-01-31]. Dostupné z: http://www.perfected.cz/mzp/

[28] PISCIOTTA, Frank a Bryan WARREN. Unique and Developing Security Challenges in Healthcare. *Security Infowatch* [online]. 2020 [cit. 2020-09-04]. Dostupné z:

https://www.securityinfowatch.com/healthcare/article/21125083/unique-and-developing-security-challenges-in-healthcare

[29] *Prevalence of violence in nursing in the czech republic* [online]. 2017 [cit. 2020-09-23]. Dostupné z: https://www.hilarispublisher.com/open-access/prevalence-of-violence-in-nursing-in-the-czech-republic-2167-1168-1000438.pdf

[30] PROCHÁZKOVÁ, Dana. Metody, nástroje a techniky pro rizikové inženýrství. Praha: ČVUT, 2011. ISBN 978-80-01-04842-9.

[31] Režimová ochrana. *Bezpečnostní poradenství Jiří Šimíček* [online]. [cit. 2020-08-24]. Dostupné z: https://www.bp-js.cz/fyzicka-ochrana/rezimova-ochrana/

[32] RUN-HIDE-FIGHT OR ALICE – IS IT ENOUGH TO KEEP EMPLOYEES SAFE? *INTEGRITY: Security Consulting & Invesigations* [online]. Chicago Office, 2021 [cit. 2021-03-21]. Dostupné z: https://www.integritysci.com/run-hide-fight-or-alice-is-it-enough-to-keep-employees-safe/

[33] SCHWARZ, Marek. *Propojení* [online]. In: Praha: Honeywell Confidential, 2020 [cit. 2021-03-28].

[34] Stopping attacks on health care. *World Health Organization* [online]. [cit. 2020-08-27]. Dostupné z: https://www.who.int/activities/stopping-attacks-on-health-care

[35] *Struktura zdravotní péče v ČR, státní a nestátní zdravotnická zařízení: Zdravotnická péče v ČR* [online]. [cit. 2020-10-05]. Dostupné z: https://is.muni.cz/el/1451/podzim2015/bp1867/um/1._seminar.pdf

[36] SURVEILLANCE SYSTEM FOR ATTACKS ON HEALTH CARE (SSA). *World Health Organization* [online]. [cit. 2020-08-27]. Dostupné z: https://extranet.who.int/ssa/LeftMenu/Index.aspx?utm_source=Stopping%20attacks%20on%20health%20care%20description&utm_medium=link&utm_campaign=Link_who

[37] ŠČUREK, Radomír. Systémy ochrany podniku - Analýzy hrozeb a rizik v security bezpečnostní praxi. Studijní texty. Ostrava: VŠB – TUO, FBI, 2017.

[38] ŠKRLA, Petr a Magda ŠKRLOVÁ. *Řízení rizik ve zdravotnických zařízení* [online]. Praha: Grada publishing, 2008 [cit. 2020-08-27]. ISBN 978-80-247-6377-4. Dostupné z: https://books.google.cz/books?hl=cs&lr=&id=mnZaAgAAQBAJ&oi=fnd&pg=PA12

&dq=identifikace+rizik&ots=v6VgcblO72&sig=YvjP69SHl30trmO7RJLyq-SduAM&redir_esc=y#v=onepage&q=identifikace%20rizik&f=false

[39] STANICE JIP (JEDNOTKA INTENZÍVNÍ PÉČE). *FNO: Fakultní nemocnice Ostrava* [online]. [cit. 2020-09-16]. Dostupné z: https://www.fno.cz/klinika-infekcniho-lekarstvi/stanice-jip-jednotka-intenzivni-pece

[40] Tísňové NO/NC tlačítko s odklopným krytem a pamětí poplachu. *Adiglobal* [online]. [cit. 2020-12-20]. Dostupné z: https://adiglobal.cz/cz/produkty110:80252/tisnove-no-nc-tlacitko-s-odklopnym-krytem-a-pameti-poplachu

[41] TOMÁŠKOVÁ, Pavla. *Analýza bezpečnostních standardů zdravotnických zařízení v České republice*. 2008. Diplomová práce. Univerzita Karlova, Fakulta humanitních studií, Katedra řízení a supervize v soc. a zdrav. organizacích. Vedoucí práce Vrzáček, Petr.

[42] ÚNIKOVÝ VÝCHOD VPRAVO. *TRAIVA: Určujeme směr k bezpečnosti* [online]. Ostrava [cit. 2021-03-21]. Dostupné z: https://www.traiva-shop.cz/bezpecnostni-tabulky/unikove-a-bezpeci/2207-unikovy-vychod-vpravo/09739/?gclid=Cj0KCQjw3duCBhCAARIsAJeFyPVj4fJTpPhEvBJt4KCOPvjISlwNG0WARTyXcYJqBhHDhLXvDWikjTQaAiUOEALw_wcB

[43] *Ústav zdravotnických informací a statistiky České republiky: 4.1.3 Počet zdravotnických zařízení v čase* [online]. Praha: ÚZIS ČR: Regionální zpravodajství Národního zdravotnického informačního systému [cit. 2021-02-19]. Dostupné z: https://reporting.uzis.cz/cr/index.php?pg=statisticke-vystupy--infrastruktura-zdravotni-pece--prehled-zdravotnickych-zarizeni--pocet-zdravotnickych-zarizeni-v-case

[44] Video Management Systems in Healthcare Facilities. *Security magazine* [online]. [cit. 2020-08-31]. Dostupné z: https://www.securitymagazine.com/articles/90348-video-management-systems-in-healthcare-facilities

[45] Video Surveillance System – What to Consider Before Investing. *Spotter security* [online]. [cit. 2020-08-31]. Dostupné z: https://www.spottersecurity.com/blog/video-surveillance-systems-what-to-consider-before-investing/

[46] *Vyhláška č. 317/2011 Sb., kterou se mění vyhláška č. 104/1997 Sb., kterou se provádí zákon o pozemních komunikacích, ve znění pozdějších předpisů* [online]. 2011 [cit. 2021-01-31]. Dostupné z: https://www.zakonyprolidi.cz/cs/2011-317.

[47] W. YORK, Tony a Don MACALISTER. *Hospital and Healthcare Security - sixth edition* [online]. 6. vydání. 2015 [cit. 2020-08-24]. ISBN 978-0-12-420048-7

[48] WHAT IS VOICE ALARM SYSTEM? *Ambient system* [online]. [cit. 2020-08-25]. Dostupné z: https://ambientsystem.eu/en/press-release-what-is-voice-alarm-system/

[49] *Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů* [online]. 2000 [cit. 2021-01-31]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-240

[50] *Zákon č. 372/2011 Sb.: Zákon o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů*. In: Praha, 2011, ročník 2011, 131/2011, 372/2011. Dostupné také z: https://www.zakonyprolidi.cz/cs/2011-372

[51] ŽIDOVÁ, Marie. *Násilí ve zdravotnických zařízeních a způsoby jeho zvládání* [online]. Bzí, 2009 [cit. 2020-08-27]. Dostupné z: https://is.cuni.cz/webapps/zzp/download/130058381. Bakalářská práce. UNIVERZITA KARLOVA V PRAZE. Vedoucí práce Mgr. Michaela Votroubková.

Seznam obrázků

Seznam grafů

Seznam tabulek

Seznam příloh